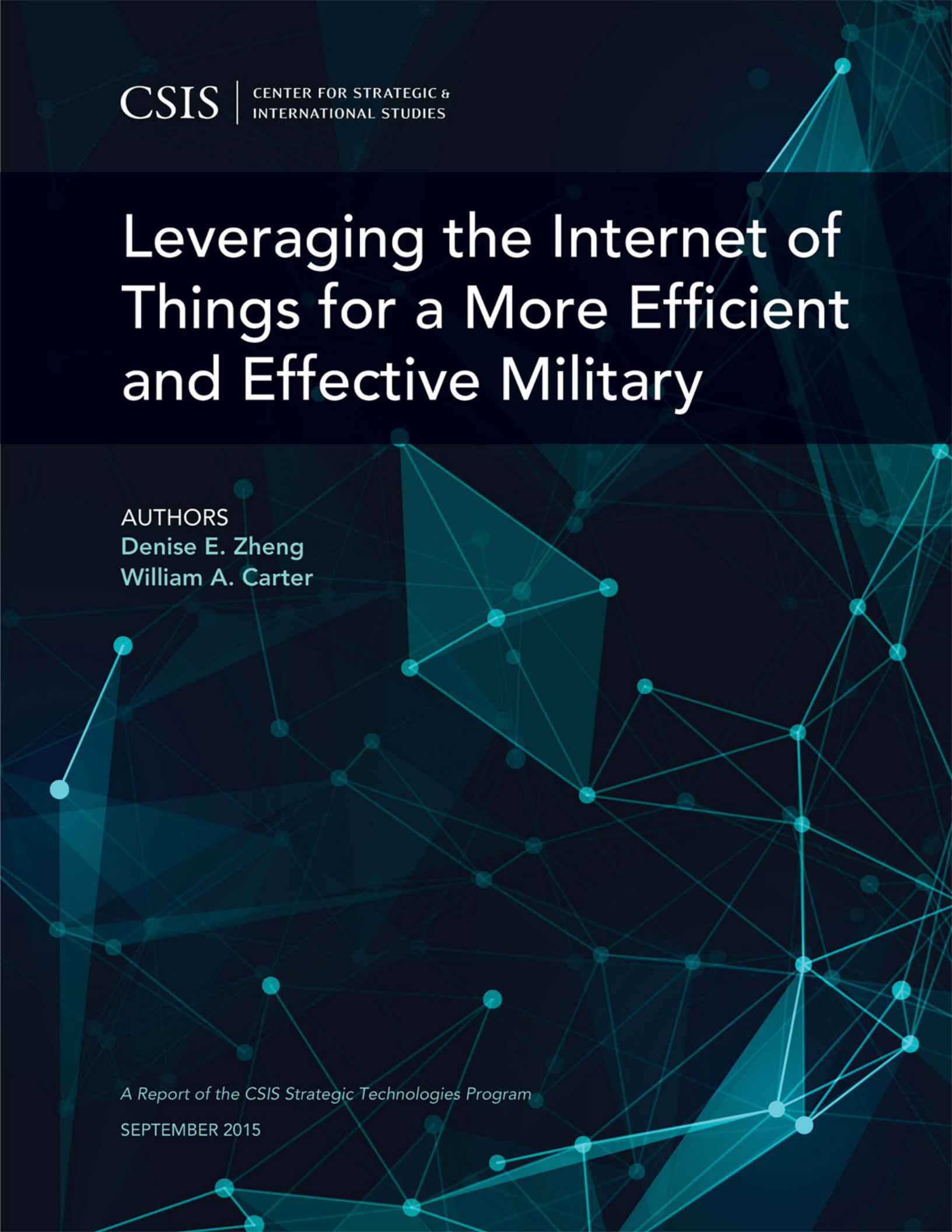
CSIS | CENTER FOR STRATEGIC & INTERNATIONAL STUDIES

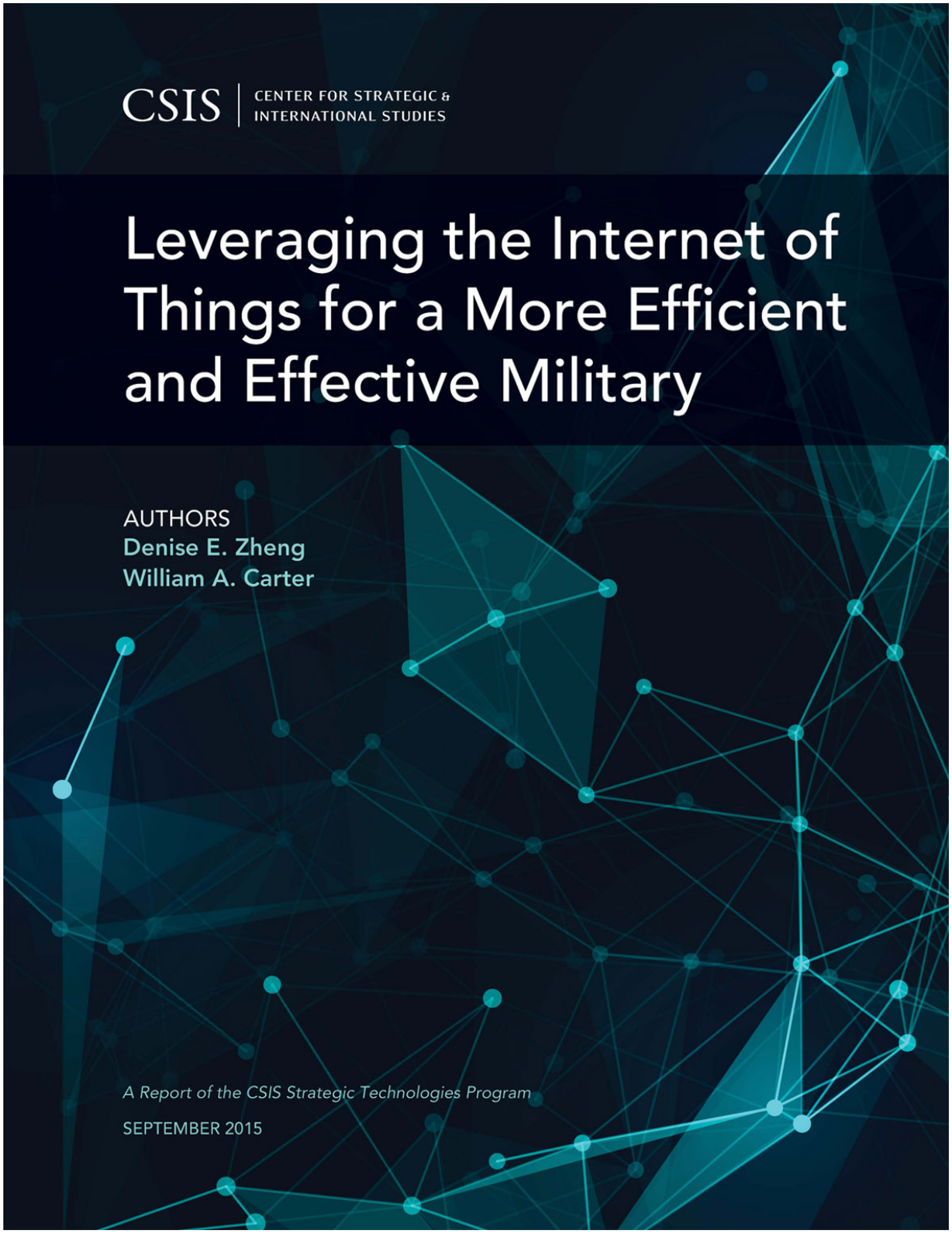
Leveraging the Internet of Things for a More Efficient and Effective Military

AUTHORS
Denise E. Zheng
William A. Carter



A Report of the CSIS Strategic Technologies Program

SEPTEMBER 2015


CSIS
CENTER FOR STRATEGIC &
INTERNATIONAL STUDIES
Leveraging the Internet of Things for a More Efficient and Effective Military
AUTHORS
Denise E. Zheng
William A. Carter
A Report of the CSIS Strategic Technologies Program
SEPTEMBER 2015

OceanofPDF.com

Leveraging the Internet of Things for a More Efficient and Effective Military

AUTHORS
Denise E. Zheng
William A. Carter

September 2015

A Report of the CSIS Strategic Technologies Program

CSIS | CENTER FOR STRATEGIC & INTERNATIONAL STUDIES

ROWMAN & LITTLEFIELD

OceanofPDF.com

ABOUT CSIS

For over 50 years, the Center for Strategic and International Studies (CSIS) has worked to develop solutions to the world's greatest policy challenges. Today, CSIS scholars are providing strategic insights and bipartisan policy solutions to help decisionmakers chart a course toward a better world.

CSIS is a nonprofit organization headquartered in Washington, D.C. The Center's 220 full-time staff and large network of affiliated scholars conduct research and analysis and develop policy initiatives that look into the future and anticipate change.

Founded at the height of the Cold War by David M. Abshire and Admiral Arleigh Burke, CSIS was dedicated to finding ways to sustain American prominence and prosperity as a force for good in the world. Since 1962, CSIS has become one of the world's preeminent international institutions focused on defense and security; regional stability; and transnational challenges ranging from energy and climate to global health and economic integration.

Former U.S. senator Sam Nunn has chaired the CSIS Board of Trustees since 1999. Former deputy secretary of defense John J. Hamre became the Center's president and chief executive officer in 2000.

CSIS does not take specific policy positions; accordingly, all views expressed herein should be understood to be solely those of the author(s).

© 2015 by the Center for Strategic and International Studies. All rights reserved.

ISBN: 978-1-4422-5890-7 (pb); 978-1-4422-5891-4 (eBook)

Center for Strategic & International Studies
1616 Rhode Island Avenue NW
Washington, DC 20036
202-887-0200 | **www.csis.org**

Rowman & Littlefield
4501 Forbes Boulevard
Lanham, MD 20706
301-459-3366 | **www.rowman.com**

OceanofPDF.com

contents

EXECUTIVE SUMMARY

INTRODUCTION

HOW THE PRIVATE SECTOR IS LEVERAGING IOT

U.S. MILITARY USE OF IOT

GAPS AND CHALLENGES

RECOMMENDATIONS

APPENDIX: SUBJECT-MATTER EXPERTS INTERVIEWED

FURTHER READING

OceanofPDF.com

i Executive Summary

The Internet of Things (IoT) is transforming the way that organizations communicate, collaborate, and coordinate everyday business and industrial processes. Adoption of IoT technologies has proven well suited to organizations that manage large numbers of assets and coordinate complex and distributed processes. From monitoring machines on a factory floor to tracking supply chains to automating sophisticated, and often dangerous, industrial processes, IoT technologies are optimizing the performance of equipment, improving efficiency, and protecting the safety of workers.

Decades ago, the U.S. Department of Defense (DoD) played a critical role in pioneering the sensor, computer networking, and communications technology that serve as the foundation of IoT. In the late 1990s, the Department articulated a vision for "network-centric" warfare that integrated three domains—physical, information, and cognitive—to enhance information sharing and collaboration. Network-centric warfare has been a driving force behind recent defense transformation and has led to the adoption of IoT-related technologies in key areas.

But today, the U.S. military is struggling to equip its workforce, civilians and warfighters alike, with the basic functions provided by commercial smartphones. DoD continues to drive innovation in advanced sensors and control systems, but it is falling behind in deployment of IoT technologies for everyday operations that have the potential to increase efficiency, effectiveness, and deliver immense cost savings across the Department.

This project set out to identify ways in which the U.S. military could better leverage IoT applications to improve efficiency and effectiveness.[1] Our research examined gaps in existing IoT component systems across the military and identified the challenges to broader deployment of IoT technologies. Our findings and recommendations are informed by in-depth interviews with 29 government and industry executives and subject-matter experts.[2]

THE CURRENT STATE OF THE MILITARY INTERNET OF THINGS

Deployment of IoT-related technologies by the military has primarily focused on combat applications. Command, Control, Communications, Computers, Intelligence, Surveillance and Reconnaissance (C4ISR) systems use millions of sensors deployed on a range of platforms to provide situational awareness to senior commanders and warfighters on the ground, on the seas, and in the air. In fire control systems, end-to-end deployment of networked sensors and digital analytics enable fully automated responses to a range of threats in real time, delivering devastating firepower with pinpoint precision.

The military has also deployed some IoT technologies in noncombat settings, improving the efficiency and effectiveness of back-end processes. The Defense Logistics Agency and Transportation Command use radio-frequency identification (RFID) tags to track shipments and manage inventories between central logistics hubs. IoT is also used in some training and simulation exercises, by networking lasers and wearable receivers to mimic live combat. DoD has also invested significantly in mobile technologies, including tactical mobile for warfighters and enterprise and other nontactical mobile programs.

However, there are significant gaps in existing and planned military IoT systems. Few military systems leverage the full IoT stack, from connected sensors to digital analytics and automated response. Data collection and sharing often depend not on networked sensors but on manual entry, and much of the data gathered across the DoD enterprise is never analyzed or put to use. Much of the value of IoT is also generated by

automation, allowing systems to react more quickly and precisely to data than can human beings, but few military systems include fully autonomous responses.

A number of obstacles stand in the way of successful development and deployment of IoT technologies across the military. Security is the most significant challenge to broader IoT adoption across the military, with the large number of simple devices and applications raising unique vulnerabilities to electronic and cyber warfare. Broader deployment of IoT technology across the military also requires investment in increased connectivity, digital analytics, and improved interoperability.

Resistance to change is a fact of life, and the military is no exception. Greater adoption of IoT will require buy-in from key stakeholders, but even the most open-minded and forward-thinking commanders can struggle to understand how to apply new technologies to existing challenges. In the private sector, IoT solutions have delivered significant cost savings for a range of commercial and industrial settings. However, the military is reluctant to spend limited budgets on up-front costs associated with development and deployment of new devices and applications for potential future savings. Culture clash between DoD and innovators in the private sector, as well as DoD's intellectual property and export restrictions, also deter some of the most innovative technology companies from collaborating with the military.

RECOMMENDATIONS

Despite the challenges of adopting IoT, there is great potential for IoT technologies to revolutionize modern warfare, leveraging data and automation to deliver greater lethality and survivability to the warfighter while reducing cost and increasing efficiency. These technologies can help the military adapt to a modern world in which adversaries are more sophisticated and capable and military budgets are shrinking.

Invest in Cost-Saving IoT Applications: Broader development and deployment of IoT applications across the military will take time; however, there are areas where the military can generate significant savings from IoT

using existing technologies and business practices available in the commercial sector.

- *Condition-Based Maintenance*: DoD should retrofit its vehicle fleet with onboard sensors to monitor engine performance and parts status, facilitating condition-based maintenance and on-demand ordering of parts and reducing unanticipated failures.
- *Real-Time Fleet Management*: Adopting IoT devices for real-time fleet management, including geolocation, status, fuel efficiency, and weight and cargo sensors, could reduce fuel costs by as much as 25 percent and increase fleet utilization by 20 percent.
- *Inventory Management*: Deploying RFID tags and standardized barcodes to track individual supplies down to the tactical level can provide real-time supply chain visibility and allow the military to order parts and supplies on demand.
- *Base Management and Energy Efficiency*: Smart thermostats have saved consumers as much as 10–15 percent on heat and cooling; even half those efficiency gains could save DoD $700 million on energy per year.[3]

Build Out IoT-Enabling Technologies: There are key technologies that DoD should invest in today to enable greater IoT deployment in the future.

- *Extend Connectivity*: The military should invest in resilient, flexible capabilities to extend Internet connectivity in denied areas, including high-altitude communications relay platforms, CubeSat (miniaturized satellite) technology, and, where appropriate, piggybacking on commercial communications satellites.
- *Common Security Overlays for COTS Devices and Applications*: The military should invest in developing new security techniques that can be applied to commercial, off-the-shelf (COTS) devices and applications, including those hosted in the cloud, focusing on investing in scalable security measures instead of securing individual systems.
- *Develop Common Standards and Protocols*: The key to delivering IoT capabilities across an enterprise as broad as DoD is a suite of common

standards and protocols that will enable integration of new IoT devices into DoD's digital ecosystem, and leverage existing systems in innovative ways.

Pursue Innovative Ways to Access Innovation: DoD should adopt commercial best practices for technology development and procurement to enable enhanced collaboration with the private sector to field, maintain, and update IoT systems quickly with the newest technologies.

- *Open Acquisitions Fairs*: The military should consider holding open technology fairs in Silicon Valley, asking the tech community how they can enhance the military mission instead of asking them to build to predetermined requirements.
- *Technology Test-Bed*: The military should consider creating a dedicated technology testbed comprised of active military personnel in a live-training environment to identify and experiment with technologies that could transform the way the military accomplishes its mission and to serve as a link between warfighters in the field and technology developers.
- *Adopt Agile Development*: Agile software development (ASD) is the common standard across innovative technology companies, emphasizing constant bilateral communication between users and developers. It allows for frequent adjustments and updates to requirements and capabilities, in contrast to traditional military contracts that emphasize formal reporting and redundant oversight.
- *Platform-as-a-Service Contracting*: The military should contract with private providers to deliver web-based services without building and maintaining the infrastructure themselves, thereby creating a more flexible framework for the provider to adjust systems to accommodate DoD preferences and update systems with the newest capabilities.

***

The Internet of Things is a tool for creating value out of data. In the private sector, it is transforming how products and services are developed and distributed, and how infrastructure is managed and maintained. The

impact of IoT on the commercial sector has been tremendous, resulting in significant improvements in efficiency and effectiveness. DoD has an opportunity to seize tremendous benefits from IoT by partnering with the private sector and adopting modern, IoT-enabled business practices.

Broader deployment of IoT in the military is not without many challenges; however, leveraging data and automation can deliver greater lethality and survivability to the warfighter while reducing cost and increasing efficiency. Greater adoption of IoT can help the military adapt to a modern world in which adversaries are more sophisticated and capable and military budgets are shrinking.

Footnotes

[1] This report is made possible by the generous support of AT&T.

[2] A list of experts interviewed for this report appears in the appendix. Information gleaned from these interviews deeply informed the report, although we did not seek explicit endorsement for the findings and recommendations from the experts interviewed.

[3] U.S. Department of Defense, Office of the Deputy Under Secretary of Defense for Installations and Environment, "Department of Defense Annual Energy Management Report Fiscal Year 2014," May 2015, 18, http://www.acq.osd.mil/ie/energy/energymgmt_report/Tab%20B%20-%20FY%202014%20AEMR_FINAL.pdf.

OceanofPDF.com

1 Introduction

The Internet of Things (IoT) describes a world in which everyday objects are embedded with tiny computers that can monitor surroundings, display information, and perform actions with some degree of autonomy. While most people think of IoT as smartphones, health and fitness monitors, and self-driving cars, it is much more. IoT is smart meters that enable better management of power and water resources across the grid, sensors and actuators that monitor and automate a factory floor, telematics used for automotive insurers to more accurately model and price risk, smart systems that monitor the performance of jet engines, and improved patient monitoring and disease diagnosis. The list of potential applications is endless.

According to researchers, IoT is estimated to reach 50 billion connected devices by 2020[4] and the potential economic impact of IoT technologies will be between $2.7 to 6.2 trillion per year by 2025[5]. Rapid growth of IoT is driven by four key developments in digital technologies. The first is the declining cost and size of ever-more-powerful sensors, controllers, and transmitters. The average cost of sensors has fallen more than 50 percent from $1.30 to $0.60 in the last decade.[6] The second is increasing Internet penetration, bandwidth, and the expansion of wireless connectivity, such as 4G LTE, Wi-Fi, and Bluetooth, which have enabled an enormous variety of devices in disparate locations to be embedded with connectivity without being tethered to a hard line Internet connection. 4G LTE, in particular, has allowed companies to network a wide range of

consumer devices, utilizing carrier aggregation, multipath propagation, and hetnets to provide greater bandwidth and efficiency and facilitate more simultaneous connections.[7] Third is the expansion of data storage and processing capacity, which has reduced cost and made it simpler to store and organize massive amounts of data. And finally, innovative software applications and analytics, including advancements in machine-learning techniques and algorithms, have enabled people and businesses to turn data into knowledge and actionable information.

These technology drivers also represent the key layers of the IoT technology stack. IoT includes sensors, embedded devices, cameras, and meters that collect data on physical and environmental conditions, such as heart rate, oncoming vehicle traffic, crop conditions, or the wear and tear on machine components. These devices then transmit data over a communication network, wired or wireless, to more powerful computers and servers that store and process the data using software applications and analytics. The device itself often has analytics and applications embedded in it to enable local processing of data. Knowledge gleaned from analyzing the collected data can be used for anomaly detection, control, prediction, and optimization of systems and processes. IoT systems are more than just sensors collecting massive amounts of data. To be a true IoT system, the data must undergo analysis and be used to effect some type of physical or virtual response.

In the 1950s, the U.S. Department of Defense (DoD) pioneered the sensor and computer networking technologies that serve as the foundation for IoT technologies as we know them today. The origins of wireless sensor network technologies were first developed by the U.S. military to detect and track Soviet submarines.[8] The Sound Surveillance System (SOSUS) was a chain of underwater listening posts throughout the Atlantic and Pacific Oceans. It consisted of a network of underwater acoustic sensors—hydrophones—connected by underwater cables to facilities on land.[9] In the 1980s, the Defense Advanced Projects Agency (DARPA) formally launched a program to develop distributed, wireless sensor networks in partnership with academic researchers at the Massachusetts Institute of Technology Lincoln Laboratory and Carnegie Mellon University. As the discipline caught on in academia and the civilian research community, the use of wireless sensor technologies spread to air and weather monitoring, and

eventually industrial applications such as power distribution, wastewater treatment, and factory automation.[10]

The Department of Defense has also played a significant role in the development of the commercial microelectronics industry. As early proponents of the miniaturization of integrated circuits, U.S. military and space agencies played an important role in enabling objects of all shapes and sizes to be embedded with tiny computer chips.[11] The military injected significant funding to support research, development, and manufacturing by commercial firms for microelectronics in the 1980s when it perceived potential decline of the industry in the United States.[12]

Perhaps most important is the critical role that the military played in developing the Internet itself. In the late 1960s through 1970s, the DoD created ARPANET, a network of computer terminals designed to enable geographically dispersed scientists to access functions and data located on different computers without the cost of travel and time. Another motivation was to design a system that would provide continuity of communications in the event of a nuclear attack. The Internet as it exists today is dramatically different than how it was initially conceived. It has evolved into a platform that has fundamentally altered the way people live, learn, and work in a manner that enables people and organizations to be more proactive and less reactive.

But today the military is struggling to equip its civilian employees, let alone forward-deployed troops, with the basic functionalities provided by commercial smartphones. Indeed, the military continues to lead in the development of some high-end applications of IoT technologies such as surveillance and reconnaissance drones, advanced sensors, and satellite communications systems, but the development and deployment of the vast majority of IoT applications are driven by the commercial sector with the military severely lagging behind.

The *Capstone Concept for Joint Operations: Joint Force 2020*[13] lays out a vision for the future Joint Force that is very different from the current state. It envisions a future in which digital collaboration technologies will enable the military to realize mission command in even more powerful ways, and mobile devices and connectivity will allow distributed commanders and staffs to collaborate as if they are colocated. Achieving this vision will require significant investment in technology, including in

IoT technologies, and changes in policies, processes, and culture across the Department.

The military has unique operational requirements that reduce its tolerance for risk. Security, safety, interoperability challenges, as well as cultural and bureaucratic hurdles stand in the way of the military's adoption of new IoT applications and modern business practices enabled by IoT technologies it has played a critical role in pioneering. IoT technologies have the potential to enable the military to achieve significant efficiencies, improve safety and delivery of services, and produce major cost savings.

There are ways in which the military is currently using IoT technologies, but our research found that the Department is not taking a thoughtful approach to laying the groundwork for broader deployment of IoT. This report outlines the primary technical, policy, and cultural challenges that stand in the way of DoD's more effectively leveraging IoT technologies at a broader scale. The report concludes with recommendations for how DoD could leverage a broader range of IoT applications to improve effectiveness and health of the warfighter and achieve cost savings across the Department.

Footnotes

[4] Lopez Research, “An Introduction to the Internet of Things (IoT),” Part 1 *The IoT Series*, November 2013, http://www.cisco.com/web/solutions/trends/iot/introduction_to_IoT_november.pdf.

[5] James Manyika et al., “Disruptive Technologies: Advances That Will Transform Life, Business, and the Global Economy,” McKinsey Global Institute, May 2013, http://www.mckinsey.com/~/media/McKinsey/dotcom/Insights%20and%20pubs/MGI/Research/Technology%20and%20Innovation/Disruptive%20technologies/MGI_Disruptive_technologies_Full_report_May2013.ashx.

[6] Goldman Sachs, “The Internet of Things: Making Sense of the Next Mega-trend,” September 3, 2014, http://www.goldmansachs.com/our-thinking/outlook/internet-of-things/iot-report.pdf.

[7] Hetnets, or heterogenous networks, are networks that provide seamless connectivity between multiple types of nodes using different protocols.

[8] Wireless sensor networks are spatially distributed autonomous sensors that monitor temperature, sound, pressure, particles, and other physical and environmental conditions.

[9] Silicon Laboratories, “The Evolution of Wireless Sensor Networks,” 2013, https://www.silabs.com/Support%20Documents/TechnicalDocs/evolution-of-wireless-sensor-networks.pdf.

[10] Ibid.

[11] Jack S. Kilby, “Turning Potential into Realities: The Invention of the Integrated Circuit,” Nobel Lecture given at Texas Instruments Incorporated, Dallas, Texas, December 8, 2000, http://www.nobelprize.org/nobel_prizes/physics/laureates/2000/kilby-lecture.pdf.

[12] Anna Slomovic, “An Analysis of Military and Commercial Microelectronics: Has DoD’s R&D Funding Had the Desired Effect?” (dissertation, Rand Graduate School, 1991), https://www.rand.org/content/dam/rand/pubs/notes/2009/N3318.pdf.

[13] U.S. Joint Chiefs of Staff, “Capstone Concept for Joint Operations: Joint Force 2020,” September 10, 2012, http://www.dtic.mil/doctrine/concepts/ccjo_jointforce2020.pdf.

OceanofPDF.com

2 How the Private Sector Is Leveraging IoT

IoT is transforming a range of different activities in the private sector and improving productivity, efficiency, and profitability. It has enabled more effective monitoring and coordination of manufacturing, supply chains, transportation systems, and the delivery of medical care, among other things. IoT is creating new business models and improving decisionmaking for companies, redefining how people and machines interact with each other.

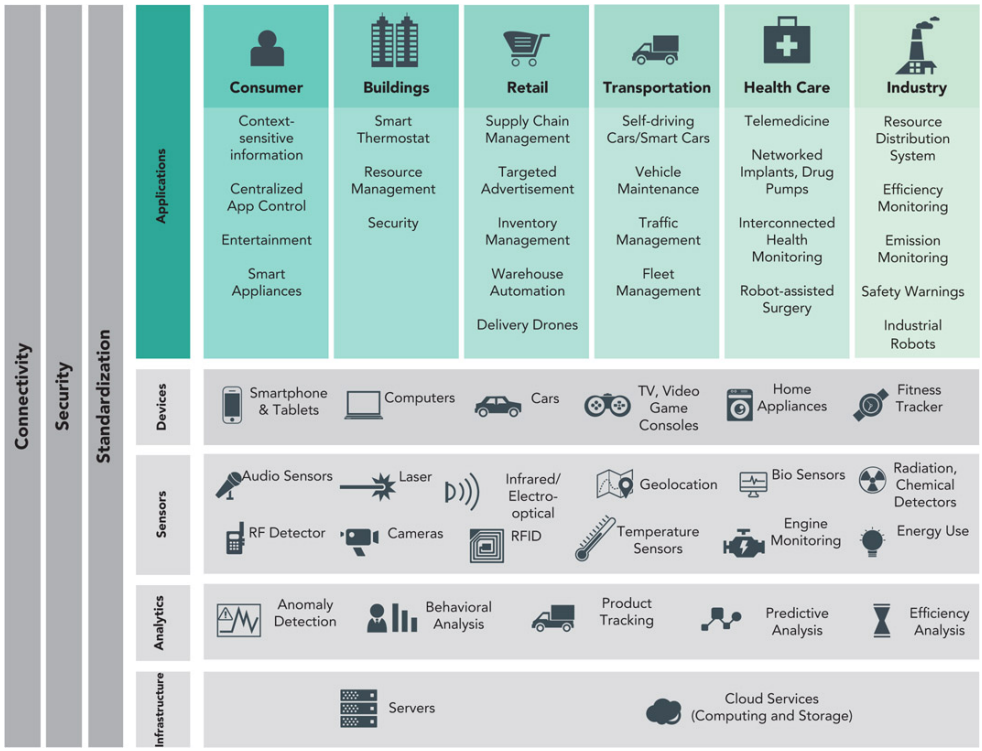
Currently, the enterprise sector is leading the adoption of IoT, consuming approximately 46 percent of IoT device shipments in 2014. This trend is largely driven by gains from operational efficiency and cost reduction.[14] Uses include factory surveillance, maintenance, operational feedback, building and facility security, energy management, and transportation. Public-sector (i.e., government) adoption lags behind but is estimated to increase significantly and potentially overtake enterprise adoption by 2019, particularly in the areas of transportation, energy management, and smart cities.[15]

Examples of IoT deployment are numerous, but four areas where IoT deployment has achieved significant benefits include aircraft maintenance, mining, energy efficiency, and inventory management. These cases are illustrative of applications that could benefit the military.

AIRCRAFT MAINTENANCE

IoT is revolutionizing the aviation industry. The modern jet engine is equipped with a variety of sensors that produce several terabytes of data per flight.[16] Combined with other inflight data, the information can improve engine performance and maintenance management to reduce fuel costs, shorten travel times, and increase efficiency.

Exhibit 1. Private Sector Tech Stack



Previously, sensor and actuator data could only be downloaded after landing, but new technology is enabling flight data to be tracked in real time by operators and analysts on the ground. Data and sophisticated analytics also enable predictive maintenance by detecting minor faults in avionics before they become problems. This enables preventative

maintenance, resulting in less downtime spent in repairs for the lifecycle of the aircraft.

For large airlines, significant cost savings can be achieved through even small reductions in jet fuel consumption. General Electric and Alitalia collaborated to use IoT to improve Alitalia's fuel efficiency through changes in flight procedures, wing flap positions, and adjustments in airspeed using sensor data. The result was improved fuel efficiency by 1.5 percent in the first year. According to industry analysts, a small 1 percent reduction in jet fuel consumption could save the global airline industry $2 billion per year.[17]

AUTOMATED MINING

IoT deployment by the mining industry has demonstrated significant improvements in safety and cost reduction. Real-time monitoring of equipment and autonomous mining systems are transforming mining operations, enabling more ore to be mined by existing infrastructure. Monitoring also lowers costs by reducing outages and maintenance, and significantly improving mine safety by reducing injuries and fatalities.

Rio Tinto's autonomous drilling systems, including tunneling and boring machines, and driverless trucks and trains extract and haul hundreds of millions of tons of material across Western Australia. Each truck is equipped with 300 to 400 sensors that produce about 4.9 terabytes of data per day.[18] From the launch of the program in 2008 to 2014, Rio Tinto autonomous trucks moved more than 300 million tons of material and effective utilization of haulage systems has increased by 10–15 percent. The autonomous equipment and driverless trucks are controlled from a Rio Tinto Remote Operations Center more than 900 miles away in Perth. Operators located at this "mission control" site manage and control operations at 15 mines, 31 pits, and 4 port terminals.[19]

Embedded sensors on equipment and vehicles provide a more precise picture of ground operations, and enable real-time monitoring of mining equipment. These technologies have improved maintenance and better performance on fuel and tires, reducing expenditure on infrastructure and machines. Data collected from equipment, vehicles, and other sensors are

analyzed at Rio Tinto's Process Excellence Center to produce real-time models and control and planning algorithms coordinate vehicle fleets to increase efficiency and reliability, and improve overall performance across the supply chain. Rio Tinto saves more than $80 million per year through more effective use of the data collected from sensors and algorithms on its copper mines alone.[20]

FACILITY ENERGY AND SECURITY MANAGEMENT

Using sensors and predictive algorithms, smart energy management systems automatically sense whether a room is occupied and adjust the temperate and lighting to better understand usage patterns and improve efficiency. According to industry analysts, IoT-based energy management systems can reduce energy use in offices by 20 percent.[21]

Digital sensors and security cameras combined with sophisticated image analysis and pattern-recognition software can enable more effective facility monitoring for security threats. Monitoring can be done remotely and reduce the cost of hiring guards to patrol small facilities.

Exhibit 2. Mine of the Future Case Study

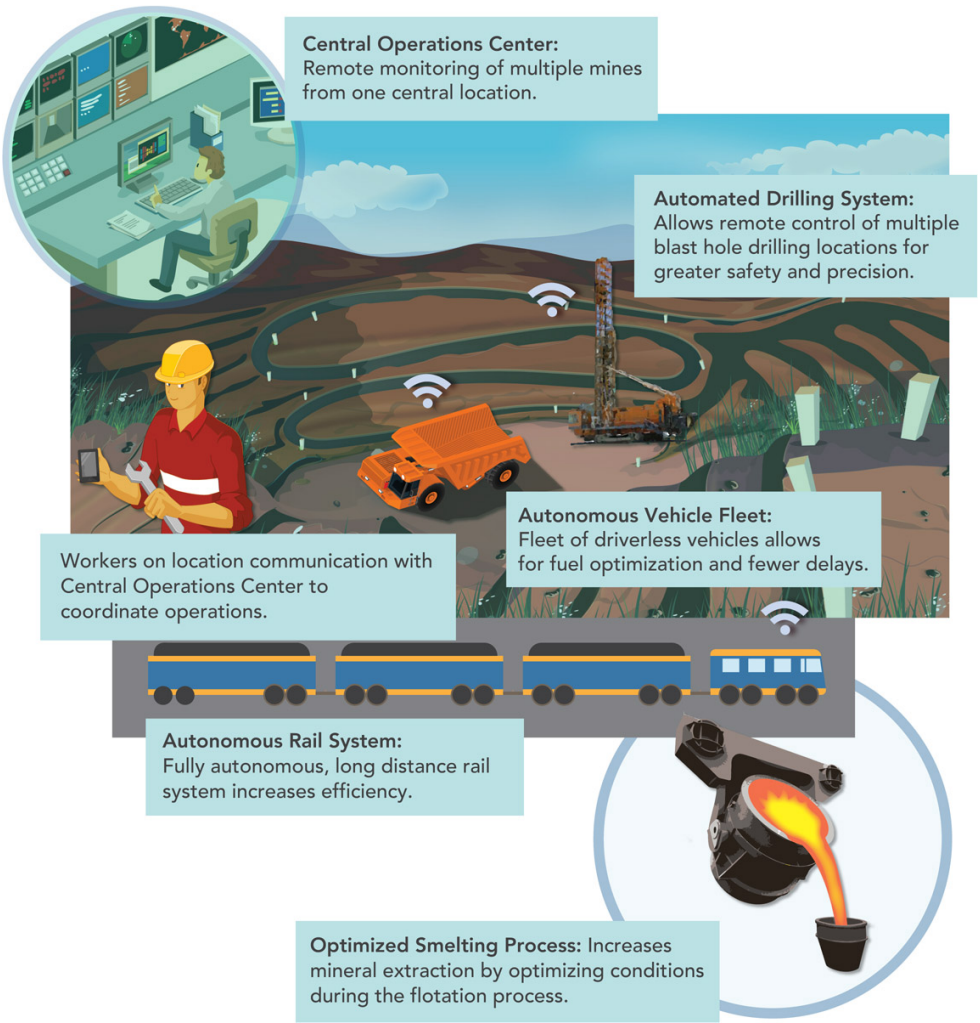
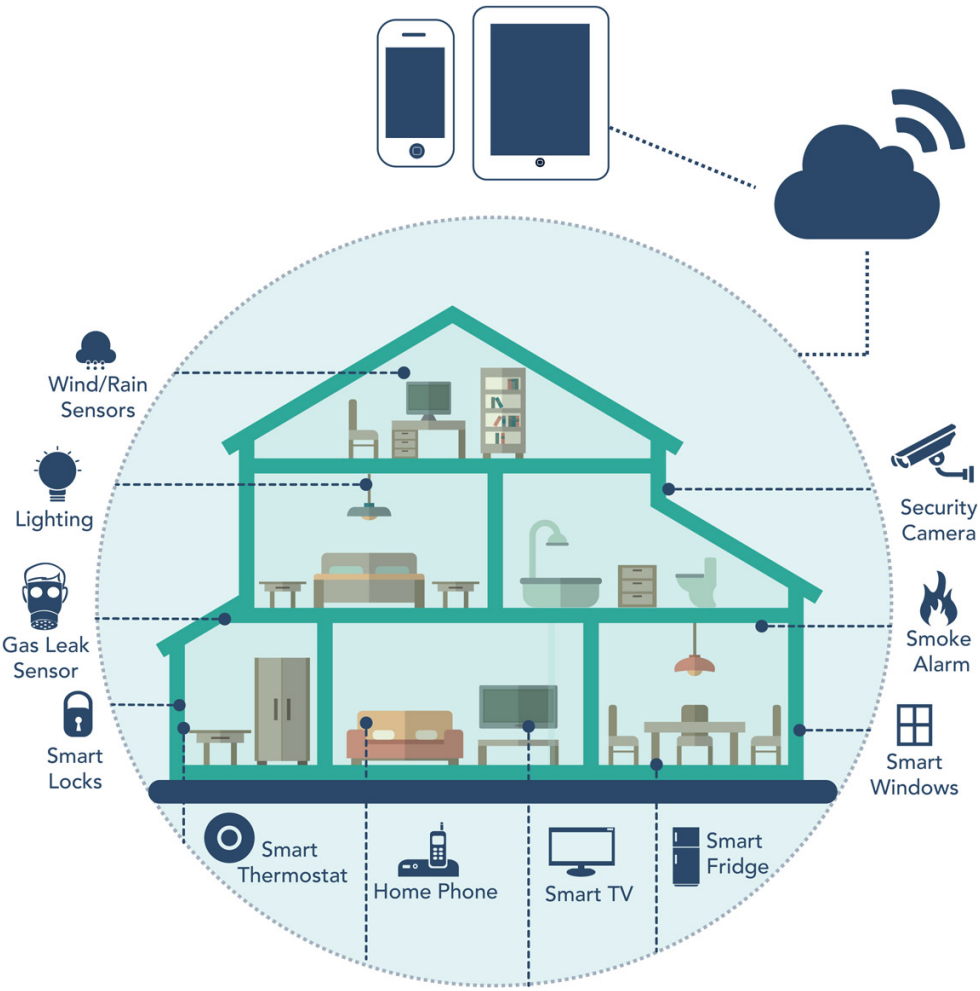

Central Operations Center: Remote monitoring of multiple mines from one central location.
Automated Drilling System: Allows remote control of multiple blast hole drilling locations for greater safety and precision.
Autonomous Vehicle Fleet: Fleet of driverless vehicles allows for fuel optimization and fewer delays.
Workers on location communication with Central Operations Center to coordinate operations.
Autonomous Rail System: Fully autonomous, long distance rail system increases efficiency.
Optimized Smelting Process: Increases mineral extraction by optimizing conditions during the flotation process.

Exhibit 3. Smart Home Case Study



Connected devices have proliferated throughout the home, improving energy efficiency, enhancing home security, and simplifying household tasks for consumers. Today virtually any home appliance can be automated and connected to the cloud, including home security systems, lights and air conditioners, TVs and entertainment systems, and even refrigerators and washers and dryers.

INVENTORY AND SUPPLY CHAIN MANAGEMENT

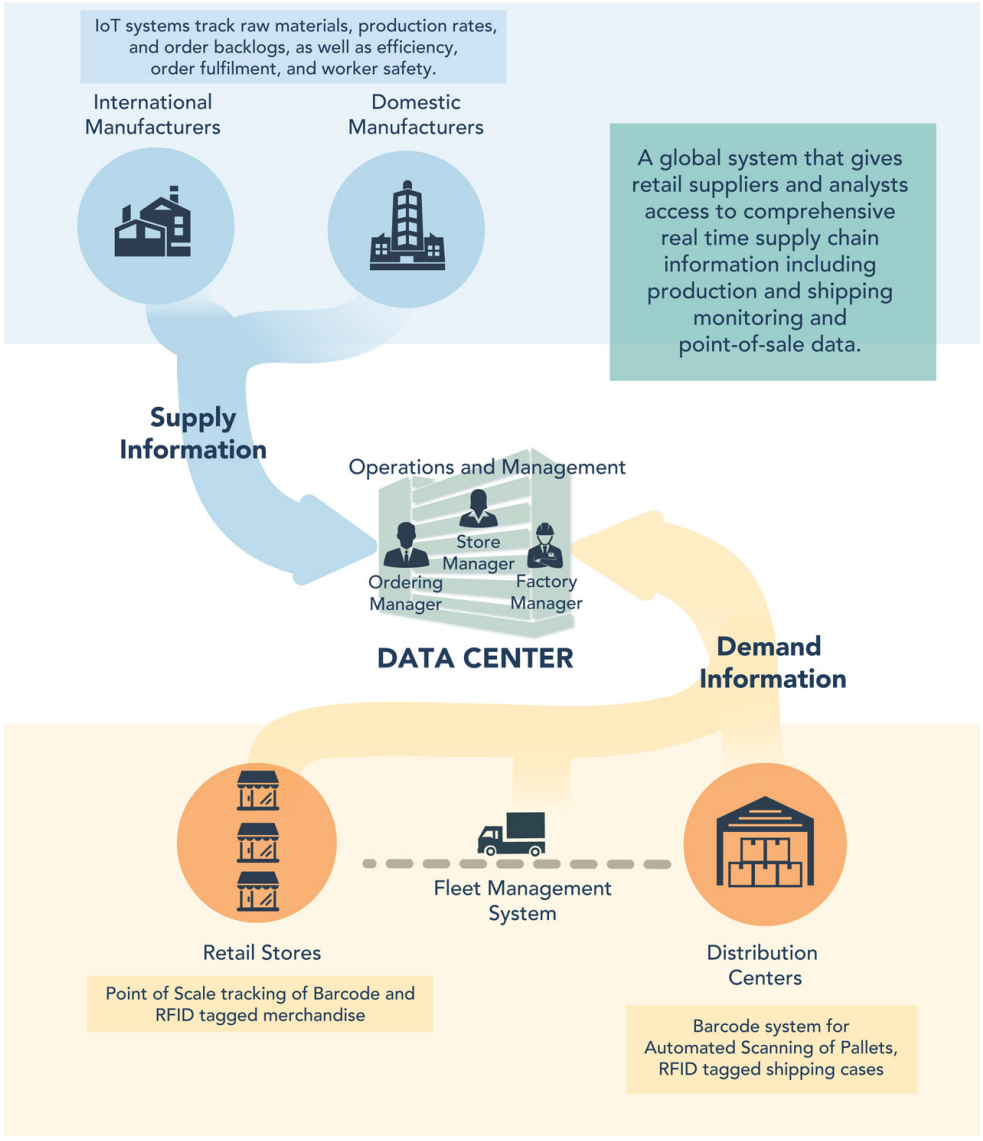
IoT technologies can optimize inventory management resulting in cost reduction, better pricing, and greater profitability. RFID tags, barcodes, and sensors can automatically monitor inventory levels by tracking the weight or height of items and triggering replenishment when supplies are low. The use of analytics with backend database systems to provide pricing and

availability data can enable smarter procurement of raw materials and finished goods. Industry analysts estimate that IoT technology could help reduce inventory-carrying costs by up to 10 percent. IoT-enabled inventory systems also help avoid delays caused by out-of-stock parts.

IoT devices can also enable tracking of shipments around the world. Shipping companies utilize IoT devices to track the position and status of containers, allowing customers to monitor containers in transit. They can also see whether the container has been opened, and sense temperature, pressure, and shocks that could affect sensitive cargo. This not only allows companies to monitor their shipments and identify potential problems, but improves accountability of shippers and suppliers.

This is only a small sample of the many ways in which the private sector is leveraging IoT to improve efficiency and effectiveness and enabling new business models. Similar improvements in performance and cost savings could be achieved if these applications were deployed across the military.

Exhibit 4. Supply Chain Case Study


IoT systems track raw materials, production rates, and order backlogs, as well as efficiency, order fulfilment, and worker safety.
International Manufacturers
Domestic Manufacturers
A global system that gives retail suppliers and analysts access to comprehensive real time supply chain information including production and shipping monitoring and point-of-sale data.
Supply Information
Operations and Management
Store Manager
Ordering Manager
Factory Manager
DATA CENTER
Demand Information
Fleet Management System
Retail Stores
Point of Scale tracking of Barcode and RFID tagged merchandise
Distribution Centers
Barcode system for Automated Scanning of Pallets, RFID tagged shipping cases

Footnotes

[14] Ross Rubin, "Here Comes the Internet of Things," *Business Insider Intelligence*, October 23, 2013, http://www.slideshare.net/marklittlewood/business-insider-iot-report.

[15] Ibid.

[16] Danny Palmer, "The Future Is Here Today: How GE Is Using the Internet of Things, Big Data and Robotics to Power Its Business," Computing.co.uk, March 12, 2015, http://www.computing.co.uk/ctg/feature/2399216/the-future-is-here-today-how-ge-is-using-the-internet-of-things-big-data-and-robotics-to-power-its-business.

[17] Morgan Stanley, "The 'Internet of Things' Is Now: Connecting the Real Economy," Blue Paper, April 3, 2014, http://www.wisburg.com/wp-content/uploads/2014/09/%EF%BC%8896-pages-2014%EF%BC%89MORGAN-STANLEY-BLUE-PAPER-THE%E2%80%98INTERNET-OF-THINGS%E2%80%99-IS-NOW-CONNECTING-THE-REAL-ECONOMY.pdf.

[18] Aimee Chanthadavong, "Rio Tinto Digs for Value in Data," ZDNet, March 2, 2015, www.zdnet.com/article/rio-tinto-digs-forvalue-in-data.

[19] Rio Tinto, "Mine of the Future—Next-generation Mining: People and Technology Working Together," 2014, http://www.riotinto.com/documents/Mine_of_The_Future_Brochure.pdf.

[20] Rio Tinto, "Delivering Greater Value for Shareholders," Presentation at the Bank of America Merrill Lynch Metals Mining & Steel Conference, March 14, 2014, http://www.riotinto.com/documents/RT_BoAML_2014_slides.pdf.

[21] James Manyika et al., "The Internet of Things: Mapping the Value beyond the Hype," McKinsey Global Institute, June 2015, http://www.mckinsey.com/insights/business_technology/the_internet_of_things_the_value_of_digitizing_the_physical_world.

OceanofPDF.com

3 U.S. Military Use of IoT

The Internet of Things is not new to the military. In the 1990s, military leaders mapped out a vision for how networks and data would transform the way that war was fought. This concept formed the foundation of "network-centric warfare."

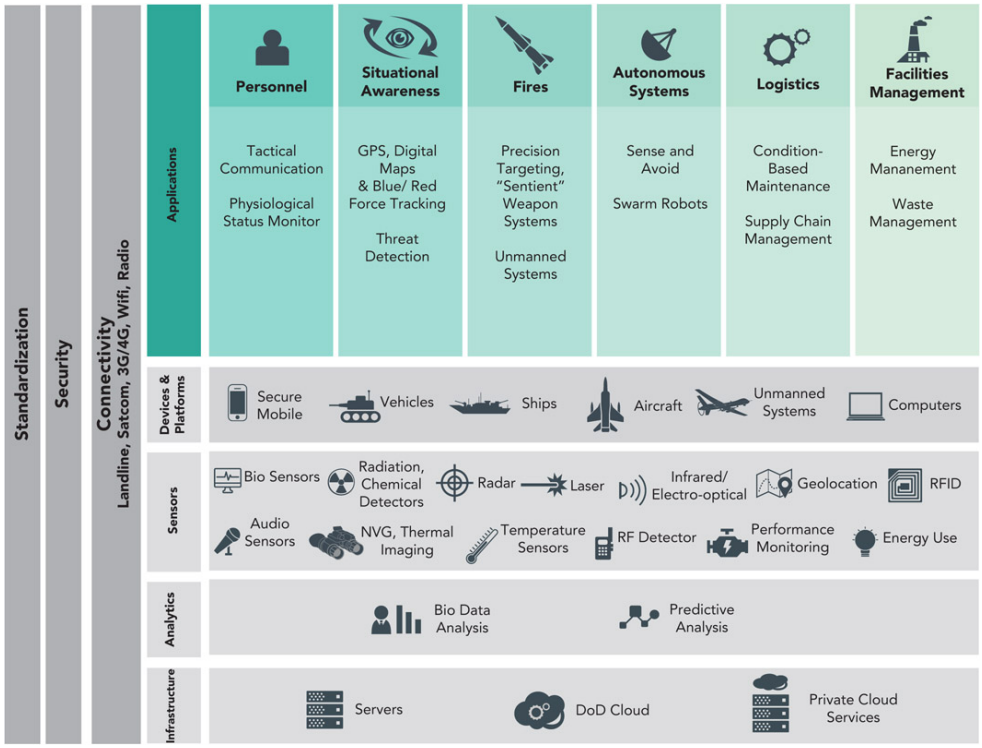
A series of books and papers authored by John Gartska, David Alberts, and Richard Hayes for the Department of Defense from 1998 to 2003 outlined the core concepts of network-centric warfare.[22] They described a model of warfare based on the integration of three domains: (1) the physical domain, where events took place and operations were conducted, generating data from sensors and human observers; (2) the information domain, in which data was transmitted and stored; and (3) the cognitive domain, in which the data was processed and analyzed.

The three domains of network-centric warfare closely mirror the modern concept of IoT, combining sensors and embedded devices, Internet connectivity, database technology, and software analytics. Network-centric warfare described the application of IoT technologies to military missions even before the concept of IoT was introduced.

To date, the deployment of IoT-related technologies by the military has primarily focused on applications for Command, Control, Communications, Computers, Intelligence, Surveillance, and Reconnaissance (C4ISR) and fire-control systems. This is driven by a predominant view across the military that sensors and networks serve first and foremost as tools to gather

and share data on the battlefield and create more effective command and control of military assets. IoT technologies have also been adopted in some applications for logistics management and training and simulation; however, deployment is limited and poorly integrated.

Exhibit 5. Military Tech Stack



COMMAND, CONTROL, COMMUNICATIONS, COMPUTERS, INTELLIGENCE, SURVEILLANCE, AND RECONNAISSANCE (C4ISR)

The military gathers data through millions of sensors deployed on a range of platforms. Radar, sonar, video, infrared, and passive RF detection data are gathered by airborne sensor platforms, surveillance satellites and unmanned aerial vehicles (UAVs), shipboard and ground stations, and

soldiers in the field and delivered to the Distributed Common Ground System (DCGS), the military's main C4ISR data-integration platform. DCGS ingests and analyzes the data and delivers information up and down the chain of command. DCGS provides a comprehensive picture of the position and disposition of friendly and enemy forces, allowing enhanced coordination and control across the battlespace.

Senior commanders are provided with comprehensive situational awareness through central operations centers that receive data feeds from platforms throughout their theater of operations. Warfighters also have access to data on activity in their area. Combat pilots receive prioritized data feeds through tactical data links (TDLs) that are integrated with data from their own sensor systems to identify threats and targets all presented through headsup displays in the cockpit.

FIRES CONTROL SYSTEMS

Fully automated systems in the military are concentrated in the fires area. These systems use sensor data to react quickly and deliver pinpoint accuracy. For example, the Navy's Aegis Combat System, an integrated fire-control system for surface ships, incorporates fully automated fires capabilities. Aegis provides command and control, as well as weapons control, to the full suite of weapons on U.S. surface ships, from shipboard artillery and torpedoes to guided cruise missiles to antimissile weapons. The AN/SPY radar system can detect, track, and steer guided munitions into as many as 100 targets at a time fully autonomously.[23]

The military is heavily invested in the use of UAVs to engage high-value targets. Pilots at ground stations use cameras and other sensors on the Predator airframe to fly the aircraft as if they were in a cockpit. Using a combination of sensors on the aircraft and information from DCGS, Predators identify targets and can engage with Hellfire missiles, using a laser designator to paint their target, allowing the missile's seeker head to hit the target with pinpoint precision.

Munitions can also be networked, allowing smart weapons to track mobile targets or be redirected in flight. A prime example is the Tomahawk Land Attack Missile (TLAM), the Navy's premier precision strike weapon.

The TLAM Block IV variant has a two-way satellite link that allows the missile to be redirected in flight to a new target, or to loiter over a target area, sending footage from its onboard camera to commanders allowing them to designate new targets and assess damage from other strikes.[24] The TLAM can also be instructed to attack any preprogrammed target, or provided with new GPS coordinates to attack.

LOGISTICS

To a limited degree, the military has deployed IoT technologies for logistics management. The Defense Logistics Agency (DLA) and Transportation Command (USTRANSCOM), which provide joint logistics management to the service branches, use IoT devices, such as RFID, to track shipments and manage inventories. For example, pallets are tagged with active and passive RFID to supplies and equipment in transit between major hubs. DLA also uses digital readers to monitor fuel levels in tanks at distribution hubs. The system then uses software analytics to adjust readings of fuel volume given environmental conditions, such as temperature. Logistics data are fed into a backend system with an interface that allows users to enter and track orders and monitor the inventory of materiel called the Integrated Data Environment/Global Transportation Network Convergence (IGC).[25]

TRAINING AND SIMULATION

IoT-related technology is also being used for military training and simulation. For example, live training “shoot houses” use cameras, motion sensors, and acoustic sensors to track soldiers during training exercises, sending data to mobile devices for trainers who can coach soldiers in real time, and producing edited video and basic statistics for troops to review after the exercise. Another example is the Multiple Integrated Laser Engagement System (MILES), which simulates live infantry combat using blank cartridges and lasers. Similar to laser tag games popular with kids and teenagers, lasers mounted on weapons send coded signals when the soldier fires a blank cartridge in simulation. If the sensors mounted on a soldier’s

clothing and equipment receive the laser signal they register a hit, activating a beeping noise indicating the soldier has been “killed.” Newer versions of MILES use connectivity and computer modeling to provide a more comprehensive training experience, simulating everything from artillery fire to weapons of mass destruction and allowing trainers to monitor exercises in real-time.

MOBILITY

DoD has launched programs across the Department to implement mobile technologies for warfighters and civilians. Separate mobile programs are being developed by the services and individual DoD agencies using different platforms, protocols, and requirements. These programs are coordinated through a working group through the DoD chief information officer (CIO) where they can share information and best practices.

The military has been developing tactical mobility for more than a decade. The Army’s Nett Warrior program and its predecessor Land Warrior have spent years developing hardened Android devices for infantry units using a proprietary version of the Android OS. These devices, which are modified from COTS Samsung Galaxy Note smartphones, link to the data-capable Rifleman Radio aim to connect soldiers in the field to a range of apps, such as 3-D maps, Blue Force Tracking, language translation, and the profiles of high-value targets (HVTs). To date, these programs have been piloted on a limited basis but broader deployment is hampered by lack of connectivity, limited functionality, and poor user experience.

The Air Force has taken a very different approach, developing apps on commercial iPads for a range of support functions. Self-trained programmers at Scott Air Force Base developed a popular drag-and-drop app to plan loads for KC-10 cargo aircraft, winning an award for government innovation in technology. The Air Force is also exploring using iPads to provide electronic equipment manuals to maintenance personnel, replacing glitchy Toughbook rugged laptops that have limited battery life.

At the Pentagon, the Defense Information System Agency’s (DISA) Mobility Program is implementing a software package for National Security Agency-approved Android devices to allow DoD executives to connect to

enterprise IT services like DoD email. The program includes secure devices that can access DoD's secret classified network, SIPRNet. Engineers are also working on security and authentication solutions to allow DoD leaders to connect to Top Secret/Sensitive Compartmented Information (TS/SCI) information on mobile devices.

Exhibit 6. Soldier of Today v. Connected Soldier of Tomorrow

Person (Today)
Communications
Smartphones equipped with 3G/4G internet for email and texting as well as phone communications.
Web Apps
Smart phone and tablet equipped with wifi, 3G/4G, camera, mic, accelerometer, digital assistant apps, media player, and GPS navigation. Can connect to other networked devices.
Smart Home
Home appliances are networked for remote control and monitoring.
Health and Fitness
Fitness Monitor: Wearable device that tracks steps taken, heart rate, sleep quality and other personal metrics.
Vehicles
Smart vehicles host a variety of apps and can be remotely controlled.
Soldier (Today)
Communications
Rifleman Radio System:
Voice and data recorder
Wideband Networking Software.
Soldier (Tomorrow)
Communications
Tactical Radio: Voice and data transmitter with wideband networking.
Situational Awareness
1. Tactical mobile devices: Host a variety of apps, share location data between individual soldiers.
2. Laser Designator Rangefinder: Utilizes laserspot imaging, celestial navigation, and a laser range-finder to generate a 3D map of the battlespace. Networked to central command for enhanced communication and awareness.
Health and Safety
1. Helmet Sensor: Measures accelerative forces for early detection of traumatic brain injury.
2. Physiological Status Monitor: Measures, stores, and transmits vital signs to soldier and command center.
Military equipment currently in development will provide enhanced situational awareness and communication to the soldier of tomorrow and allow his/her health to be monitered in real time.

Footnotes

[22] David S. Alberts et al., *Understanding Information Age Warfare* (Washington, DC: Command and Control Research Program, August 2001), http://www.dodccrp.org/files/Alberts_UIAW.pdf; David S. Alberts, John J. Garstka, and Frederick P. Stein, *Network Centric Warfare: Developing and Leveraging Information Superiority 2nd ed*. (Washington, DC: Command and Control Research Program, August 1999), http://dodccrp.org/files/Alberts_NCW.pdf; and David S. Alberts and Richard E. Hayes, *Power to the Edge: Command Control in the Information Age* (Washington, DC: Command and Control Research Program, June 2003), http://www.dodccrp.org/files/Alberts_Power.pdf.

[23] "Aegis Combat System," Navysite.de, accessed June 29, 2015, http://navysite.de/weapons/aegis.htm.

[24] Naval Air Systems Command, "Tomahawk Data Sheet," accessed June 29, 2015, http://www.navair.navy.mil/index.cfm?fuseaction=home.display&key=F4E98B0F-33F5-413B-9FAE-8B8F7C5F0766.

[25] Defense Logistics Agency, "IDE/GTN Convergence," accessed June 29, 2015, http://www.dla.mil/informationoperations/pages/IGC.aspx.

OceanofPDF.com

4 Gaps and Challenges

While the military has deployed a range of IoT-related technologies, there are significant gaps in existing and planned systems. IoT is an ecosystem of technologies that generates, shares, analyzes, and creates value from data. The military has millions of sensors connected through an extensive network infrastructure, but few systems leverage the full IoT stack, from connected sensors to digital analytics and automated responses. The military has also developed and deployed IoT-related technologies in segregated "stovepipes," making it difficult to secure and limiting the ability to communicate across systems and generate economies of scale or synergies from different types of data.

- **Data collection is dependent on manual entry**: Many DoD data integration systems rely on manual data entry, particularly in the logistics area. Bulk supplies are tracked by DLA and USTRANSCOM between major hubs using RFID tags, but when supplies are broken down and distributed beyond the central hubs, tracking becomes a manual exercise. Supply officers sign for orders on paper and enter serial numbers into computer terminals by hand. This approach is burdensome for logistics officers in the field, and poses significant risk of human error.
- **Limited processing of existing data**: One of the largest gaps in DoD's data ecosystem is digital analytics. Sensors and embedded devices collect massive amounts of information, but the data are often never

processed or analyzed. As a result, much of the information is never used; as for the information that is used, often a human being manually analyzes it and converts the data into a usable form for end-users. Dependence on manual processing can cause significant delays in getting important information to the people who can act on it, causing missions to stall or fail, or forcing leaders to make decisions without all the relevant facts.

- **Lack of automation**: Automation is the ultimate expression of IoT. Fully IoT applications leverage sensors and digital analytics to generate automated responses. IoT-related technologies that have been deployed by the military lack automation. For example, most deployed unmanned systems are not autonomous but remotely controlled by human operators. Automating rote processes can significantly enhance the lethality and survivability of warfighters and the efficiency of DoD operations, reducing the number of human beings needed to complete a task, limiting opportunities for human error, and improving reaction times.
- **Fragmented IT architecture**: The largest problem across the military's technology systems is fragmentation. The military lacks a cohesive IT architecture that can support IoT that is efficient and defensible. IT systems from across the armed services and DoD agencies are connected to DoD networks, but are developed independently and to different requirements. Often, multiple services are involved in an operation, or multiple agencies are involved in a process, but information has to be passed between their stovepiped systems manually, which is inefficient and allows for human error. Fragmentation across DoD's IT architectures complicates the development and use of common security protocols and practices across DoD networks.

Obstacles stand in the way of successful development and deployment of IoT technologies across the military, including security risks, technical limitations, and cultural barriers.

SECURITY RISKS

The single most important challenge for IoT implementation across the military is security. IoT can be used to collect and transmit data on the position, disposition, and movements of troops and materiel. As the Defense Science Board noted in a 2013 report, if DoD networks are compromised, "U.S. guns, missiles, and bombs may not fire, or may be directed against our own troops. Resupply, including food, water, ammunition, and fuel may not arrive when or where needed."[26]

The concern is that inadequately secured networks can provide the enemy with intelligence on troop disposition, the deployment of supplies and support units, and the red force intelligence available to U.S. commanders, allowing the adversary to anticipate the movements of U.S. forces. There is also concern about potential manipulation or disruption of data flows between units, altering the data to deliver a misleading picture of the tactical landscape to commanders or of the needs of troops to their headquarters and support units. Finally, security vulnerabilities could allow enemies to take control of or disable automated systems, preventing units from carrying out their mission or even using our own assets against us.

- **Device and Network Security**: The value of IoT is derived in large part from the ubiquity of IoT devices and applications and the connections between them. This creates a massive web of potential entry points for cyber attackers. These systems also depend on connectivity and backbone storage and processing to function, creating points of failure vulnerable to attack. The sheer number of nodes in the network makes it hard to ensure their security. One of the best ways to enhance the security of complex networks is to limit the number of nodes that an attacker can access from any given entry point. However, this approach to secure network architecture is fundamentally at odds with IoT, which generates much of its value from the integration of systems and data. Securing the range of devices in the Internet of Things is also difficult. Many IoT devices are small and have limited capacity, have no human interface or interaction, and depend on real-time integration of data. This complicates traditional approaches to security like compartmentalized architecture, advanced encryption, and multiple authentication, which can slow down or prevent the exchange of data between devices and systems on the network, require

more computing power on devices to decrypt data or authenticate regularly, or require human input for authentication.

- **Insider Threats and User Error**: With over 3 million employees in the DoD, including civilians, active and reserve military, and the National Guard, insider threats are a major concern. Exercising good cyber hygiene is a challenge for all large organizations. Programs to educate users on cyber risks can help, but a single mistake from a single user can allow an attacker to gain access to the system using relatively unsophisticated methods.
- **Electronic Warfare**: Another challenge to IoT implementation is that it makes systems vulnerable to electronic warfare. Most IoT technologies communicate wirelessly on radio frequencies. Adversaries can use relatively unsophisticated methods like RF jamming to block these signals, rendering the devices unable to communicate with backbone infrastructure. Wireless connections also raise the risk of exposing the positions of U.S. troops through RF emissions. Essentially, transmitting devices can serve as a beacon detectable by any radio receiver within range. Triangulation of the emissions from transmitters can compromise the location of soldiers or vehicles.
- **Automation as a Threat Multiplier**: IoT is in large part about ubiquity and automation, and these characteristics exacerbate DoD's security challenges. The volume of devices, networks, infrastructure, and data comprising IoT makes security a major challenge. Automation of equipment and vehicles extends the reach of cyber threats into the physical domain, allowing them to move beyond disrupting systems and sowing confusion to causing physical damage.

TECHNICAL LIMITATIONS

Broader deployment of IoT technology across the military will require investment in several technical enablers. Currently, the military does not have sufficient network connectivity, particularly on the battlefield, to support broader IoT deployment. Data analytics, process capacity, and lack of interoperability are additional limiting factors.

- **Connectivity**: The military currently lacks the network infrastructure necessary to handle the massive flow of data that would be generated by a broad military IoT, much less process and distribute that data. To make effective use of IoT devices, those devices must be able to connect to global networks to transmit sensor data and receive actionable analytics. Delivering secure and reliable network access is a challenge in forward operating environments, requiring the military to invest significant resources in local infrastructure.
- **Digital Analytics**: Significant investments in infrastructure and analytical software are needed to handle the enormous volume of data generated from IoT devices that need to be transferred, stored, and analyzed. Many IoT applications depend on real-time analysis of sensor data to enable automated responses. Other functions process and condense data into simple, intuitive interfaces that allow humans to leverage big data in convenient ways. Developing analytical software that can process the massive quantities of data generated by millions of sensors across DoD in real-time is difficult, and requires more flexible acquisition processes that allow DoD to integrate the most cutting-edge software quickly and efficiently. Without digital processing, the sheer volume of data is overwhelming, causing "data overload," which hurts efficiency and operations instead of strengthening them.
- **Interoperability**: Making sure that all of these systems are interoperable is another challenge. Many military systems use hardware and protocols that are specifically designed not to talk to each other. Leveraging the full value of IoT is about maximizing the number of nodes and connections in the data ecosystem, requiring a common set of standards and protocols to allow systems to talk to each other.

CULTURAL BARRIERS

Cultural hurdles complicate the deployment of IoT technologies by the military. Soldiers and commanders hesitate to invest their money, time, and energy in new ways of accomplishing missions that they are already

accomplishing today, even if new methods are more efficient or effective. Companies and innovators may see little benefit in catering to the complex and onerous requirements of DoD, which is a small and demanding customer relative to commercial markets.

- **Buy-In from Key Stakeholders**: Resistance to change is a fact of life, and the military is no exception. Truly innovative solutions often appear "newfangled" to senior officials who did not grow up in the Internet age. Even the most open-minded and forward-thinking commanders can struggle to understand how to apply new technologies to old challenges. At the user level, new technologies and approaches can also run into resistance from career servicemen who have established routines over decades to accomplish their mission. For example, the Marine Corps deployed the Global Combat Support System to manage their supply chains, but battalion logistics officers have been slow to adopt it. While the system depends on data from deployed units to inform decisionmakers at all levels of the command structure, officers in the field know what they have from walking the yards, and see little value in engaging with a digital system. This effect is exacerbated by the mixed track record of military IT systems, which often "brief well but don't perform out in the field." Many soldiers and commanders have been burned before by IT systems that promise impressive new capabilities and dramatic improvements in efficiency, but are difficult to operate or have limited functionality.
- **Spend Today to Save Tomorrow**: One of the largest constraints on military adoption of IoT is the current budget environment. Many IoT solutions generate significant long-term savings, but have up-front costs associated with the development and deployment of new devices and applications. The military is reluctant to invest today's limited budgets in what they view as hypothetical future savings. This attitude is compounded by experiences of many commanders with DoD's IT efforts that did not meet expectations.
- **Reliance on Humans in the Loop**: In the military, redundancy is often viewed as synonymous with resiliency. Many military leaders are wary of putting soldiers' lives in the hands of computers, and prefer to have analog and manual fallback options in case technology fails. This raises issues for IoT adoption, which often generates efficiencies by

reducing the role of human beings in processes in order to leverage the speed and accuracy of digital systems.

- **Culture Clash with Technology Innovators**: In order to develop new military IoT solutions, the military must partner with innovators in the private sector. However, many innovators in the tech industry balk at the culture of secrecy and politics driving military acquisitions, and at the administrative hurdles of complying with labyrinthine defense acquisition regulations. The defense acquisitions establishment is hesitant to embrace Silicon Valley's culture of experimentation and failure. Where venture capitalists make high-risk investments for one high-return payoff, even small failures or cost overruns can hurt an acquisition executive's chances for promotion or provide an avenue for political leaders to attack the Department.
- **Intellectual Property Rights and Export Controls**: Innovators' willingness to work with DoD is also undermined by restrictions on intellectual property rights for inventions developed in part with DoD funding. An intellectual property system that allows companies and individuals to protect and commercialize their inventions is a bedrock for innovation. Under current law, the government owns technology or intellectual property developed with DoD funds, and it has the right to share it with whomever it wants. The United States also has the authority to allow other contractors to manufacture and use the patented invention "for or on behalf" of the government without obtaining a license from or compensating the patent holder. An inventor who develops an idea for a new IoT product is faced with a choice—working with private investors to build a product and parlay that intellectual property into an IPO or a lucrative buyout, or expending time and resources on a product for DoD that offers thin margins built into government R&D contracts. Export controls also discourage private innovators from working with DoD. When the military buys a new technology, it is classified as a military or dual-use technology and becomes subject to export controls. Compared to the global market, DoD is a tiny customer. This is particularly true for IoT systems, which often have significant commercial applications as well as defense applications. Private tech companies may not want to cut

off their access to the larger and potentially more lucrative consumer IoT market by partnering with DoD.

Footnotes

[26] Defense Science Board, “Resilient Military Systems and the Advanced Cyber Threat,” Office of the Under Secretary of Defense for Acquisition, Technology and Logistics, January 2013, http://www.acq.osd.mil/dsb/reports/ResilientMilitarySystems.CyberThreat.pdf.

OceanofPDF.com

5 Recommendations

Despite the challenges of adopting IoT for the military, connected devices promise to revolutionize modern warfare, leveraging data and automation to deliver greater lethality and survivability to the warfighter while reducing cost and increasing efficiency. Technology can help the military adapt to a modern world in which adversaries are more sophisticated and capable and military budgets are shrinking. IoT devices can gather more data, facilitate more complex analysis and faster reactions, and reduce human error, delivering more precise and efficient military capabilities. Automation can also help reduce personnel costs, the fastest-growing component of the DoD budget, helping to cope with today's austere budget environment and deliver more capability per dollar to the warfighter in the field. This translates into a greater ability to deny and defeat enemies, and to protect U.S. troops and bring them home whole.

While it will take time for broader development and deployment of IoT applications across the military, there are functions in which the military can benefit from IoT using existing technology and business practices available in the commercial sector. There are also technologies that the military can invest in today to enable greater IoT deployment in the future. Unlocking the potential of these investments will require adopting new procurement and contracting procedures to access private-sector innovation and ensure that military technologies keep up with their private-sector counterparts.

1. Invest in Cost-Saving IoT Applications: Enhanced Logistics Management

Condition-Based Maintenance

The first major change that the military can make today is to retrofit its fleet of vehicles with onboard sensors to monitor engine performance. The Condition-Based Maintenance Plus initiative, launched by the Department of Defense in 2007, has led to the instrumentation of new large platforms like the F-22 and F-35 fighter jets, as well as many components of naval vessels, but has not been implemented in legacy platforms or smaller vehicles like helicopters and ground vehicles.

While instrumenting vehicles for condition-based maintenance (CBM) carries an up-front cost, it can enable significant long-term savings by transforming business processes across the logistics enterprise. For example, it can shrink maintenance staff, facilitate on-demand ordering of parts, reduce unanticipated part failures or unnecessary part replacement based on maintenance schedules, and enable logistics officers to better anticipate the demands of their supply chains.

The military has an opportunity to take advantage of existing systems to enable CBM, using COTS sensor systems and software deployed in the auto and industrial sectors to reduce cost, and piggybacking performance data on existing data links like Blue Force Tracker transponders, already in place on many military vehicles to limit new security risks.

Real-Time Fleet Management

The military should also consider adopting IoT technologies to manage nontactical vehicle fleets, including sensors for real-time GPS tracking, speed and engine status, total engine hours, fuel efficiency, and weight and cargo. Private companies already widely use Fleet Management Systems (FMS) to monitor and manage their fleets using common protocols like the Fleet Management Standard, established in 2002 by six major truck manufacturers to allow different vehicles and FMS to talk to each other. Telogis, which builds engine-monitoring systems for GM vehicles, estimates that its smart engine systems reduce fuel costs by 25 percent and idle time by 30 percent, and increase fleet utilization by 20 percent and

workforce productivity by 15 percent.[27] Using these systems, the military may be able to optimize the size and composition of its fleets, as well as their dispatching and utilization. IoT-enabled fleet management also improves accountability, providing granular data to fleet managers to monitor user activity.

Inventory Management

TRANSCOM already uses RFID trackers to monitor palletized shipments among major transit hubs, but extending supply chain visibility to the end-user level has significant advantages as well. The military can generate significant efficiencies by deploying RFID tags and standardized barcodes to track individual supplies down to the tactical level. These can be paired with a basic app that allows the logistics officer to select the operation being performed on the equipment— whether it's being shipped, transferred, deployed, consumed, etc.—to extend real-time supply chain visibility to the service level and simplify logistics management for operational units.

When troops need a piece of equipment, logistics officers can use the system to identify the nearest unit that has what they need and the most efficient way to deliver it, and can track the order as it is delivered to them. Real-time supply chain visibility and predictive analytics can allow the military to order parts and supplies on demand instead of stockpiling and bulk ordering. It can also increase accountability and help reduce losses and theft of military equipment. For example, a Naval Criminal Investigative Service (NCIS) report determined that the Navy's Joint Improvised Explosive Device Defeat Organization (JIEDDO) lost tens of millions of dollars' worth of IED detection equipment that later ended up on eBay because field units had poor control and oversight of their equipment.[28]

Base Management and Energy Efficiency

Commercial companies are developing a range of applications that connect devices in the user's home, allowing them to manage systems within their homes autonomously or from their mobile phone. One highly successful application has been in networked lights and thermostats, allowing users to reduce their energy consumption, saving them money and reducing their environmental footprint. According to Nest, a company that

makes commercial smart thermostats, users saved 10–12 percent on heat and 15 percent on cooling in 2014.[29] DoD spent $14 billion on facilities energy needs in FY2014, and reducing that by just 5 percent would save $700 million on energy per year, a significant decrease in the military's energy costs.[30]

2. Build Out IoT-Enabling Technologies

Commercial Satellites for Military Communications

The military should invest in resilient, flexible technologies to deliver Internet connectivity in denied areas. In the short term, developing security protocols to carry secure military communications on commercial satellites will expand the constellation of communications satellites available to military personnel in the field. It will also complicate the equation for enemies that might use disruptive, but not destructive, antisatellite weapons like directed-energy weapons, cyber weapons, and jamming technologies to deny the U.S. military capabilities in situations that fall short of full-scale war.

High-Altitude Communications Relay Platforms

Another technology that can deliver mobile, persistent connectivity is high-altitude platforms (HAPs), drones that operate above the range of most weapons systems that can be equipped with communications relays. HAPs have many advantages over alternative systems. Like satellites, they are mobile, and can provide connectivity over wide areas. However, unlike satellites, which eventually age and become defunct, HAPs can be recovered and reequipped, allowing them to be upgraded and enhanced as communications technologies evolve. They also have significant advantages over manned communications platforms like the Battlefield Airborne Communications Node (BACN) in use by the Air Force, as they can stay airborne continuously for long periods. The military has deployed four EQ-4B Global Hawk Drones with the BACN system, but will need significantly greater capacity to deliver connectivity to a full suite of connected devices across multiple operating theaters.

CubeSat Technology

In the longer term, the military should invest in CubeSat technology, developing large numbers of small satellites that can be deployed in large numbers to create highly capable constellations. Smaller satellites provide a potentially more resilient capability, since it is harder to destroy or disable dozens of small satellites than a single large satellite. Production is also faster than large satellites, and they can be launched into orbit in clusters or piggybacked on other loads. By reducing periods between satellite passes, small satellites also provide for more consistent connectivity than a single large satellite. Furthermore, in orbiting the planet they serve multiple theaters of operations, whereas fixed ground stations must be installed and disassembled as operations move to different areas.

Develop Security Overlays for Commercial Devices and Applications

Mobile devices increasingly serve as the hub that connects IoT systems to their users. Developing and maintaining proprietary devices for military applications imposes significant costs and delays on the procurement process. The government is developing security measures that would allow secure communications on COTS mobile devices; for example, the NSA has its Commercial Solutions for Classified (CSfC) Program and the Department of Defense has its DoD Mobility Classified Capability (DMCC) Program. While these programs provide a good base on which to develop secure systems for COTS platforms, it is limited to a short list of NSA-approved devices, and deployed to a small number of senior DoD officials. A few hundred devices have been deployed in the DMCC program, while more than 2 million civilians and active service members work for DoD. The program is also implemented through a cumbersome process that senior defense officials acknowledge is not readily scalable.[31]

The military should invest in developing new security techniques that can be applied to COTS devices and the applications supporting such devices in the cloud, focusing on investing in security protocols that can be applied to devices and apps instead of building individual systems securely. This approach will give DoD greater leverage in their IoT investments, allowing them to access more capability per dollar spent on proprietary research and development.

Develop Common Standards and Protocols to Enable Fast Adoption and Integration of New Capabilities

Cloud computing and digital analysis software are essential to maximizing the value of IoT systems. Cloud architecture allows for efficient allocation of computing resources, while digital analytics facilitates real-time responses to data. The key to delivering these capabilities across an enterprise as broad as DoD is a suite of common standards and protocols for hardware and software to connect and operate digital systems. One of the key weaknesses of legacy DoD systems is their lack of interoperability. This significantly limits the ability to integrate new platforms into DoD's digital ecosystem, and to leverage existing systems in innovative ways.

DoD recognizes this imperative, and is working to implement a cohesive digital architecture through the Joint Information Environment (JIE) initiative. The JIE is currently being implemented by DISA to consolidate infrastructure, enhance information security, provide global access to digital services, and facilitate collaboration within DoD and with partner organizations.[32] Common standards facilitate modular architecture, allowing individual components of the network to be easily updated and replaced as technology evolves, and also provide a simple template to which designers can tailor systems for military use.

3. Pursue Innovative Ways to Access Innovation

Traditional military acquisitions are a long and complex process, and ill-suited to the quickly evolving area of IoT technologies. Catching up with private-sector IoT applications will involve further adoption of COTS technologies and enhanced collaboration with the private sector to field, maintain, and update IoT systems quickly with the newest technologies. To accomplish this, the military needs to adopt best practices for technology development and acquisitions from the private sector. In particular, DoD should adopt a bottom-up model of innovation and procurement, crowd-sourcing creativity from the private sector and from the warfighter in the field, and pushing ownership of acquisition decisions and preferences from executives to the end-user, the warfighter.

Open Acquisition Fairs

Open acquisition fairs for new technologies could provide an opportunity to tap into new sources of innovation and revolutionary new business processes developed by the private sector. Traditional military acquisitions start with the identification of requirements by the military, which are then submitted to the defense industry to solicit proposals. However, innovators have often driven the commercial Internet of Things, who imagine creative new technologies and applications and then shop them to potential investors for further development. The military should embrace this open approach by holding open military technology fairs in Silicon Valley, asking members of the tech community how they can enhance the military mission instead of asking them to build to predetermined requirements. Soliciting unconstrained creativity from innovators can open DoD to genuinely revolutionary ways of accomplishing the mission that warfighters and acquisition executives might not think of on their own.

Technology Test Bed

The tech fairs could be complemented by the establishment of a test bed, perhaps based in Silicon Valley, dedicated exclusively to identifying and experimenting with technologies that could transform the way the military accomplishes its mission. This test bed would be composed of active military personnel in a live training environment, whose focus would be experimenting with ways to use IoT devices and applications in creative new ways to accomplish military missions. Their goal would be twofold: first, to learn and experiment with new devices and applications to identify those with potential military applications; and second, to identify completely new strategies, tactics, and methods of accomplishing missions using commercial technologies. This unit could also serve as the link between warfighters in the field and technology developers, soliciting suggestions for new systems and modifications to existing systems from soldiers and sharing them with the tech community.

Adopt Agile Software Development Practices Used in the Private Sector

Private tech companies use Agile Software Development methods that emphasize constant bilateral communication between users and developers. Agile development enables frequent adjustments and updates to requirements and capabilities. This is inconsistent with military procurement practices that dictate strict requirements that involve complex and time-consuming processes to amend.

Adopting Agile Software Development methods requires changing contract structures and the way that the military engages with its developers. Contract structures that facilitate quick and frequent adjustments to development plans to accommodate new needs and capabilities are essential. Even more important, however, is creating environments in which developers have constant access to end-users, meaning active soldiers and not just acquisition executives. A core principle of Agile Software Development is the importance of face-to-face communication. These DoD end-users should engage with developers and engineers to experiment with and test systems as they are developed and provide feedback, instead of following a typical military development program in which experts and end-users are brought in late in the process to test and evaluate largely complete systems.

Platform-as-a-Service Contracting

Platform-as-a-Service (PaaS) contracting is another way for the military to improve its access to the most advanced technologies and keep its capabilities up-to-date with the latest private-sector advances. Under PaaS contracts, the military contracts with a private provider to deliver web-based services without building and maintaining the infrastructure itself. This approach provides a more flexible framework for the provider to adjust its systems to accommodate user preferences and update its systems with the newest capabilities without going through the complex process of implementing “material changes” to traditional fixed contracts for military platforms.

PaaS also provides a more scalable way for the military to access computing resources. Adopting PaaS carries risks for the military, and requires private contractors to implement additional security procedures to support sensitive and classified government data. However, other government agencies, including the NSA and CIA, use PaaS contractors.

They can provide a model for how to manage these risks effectively through layered security measures and clear security guidelines for contractors, delivering enhanced capabilities that are difficult to maintain under traditional military contracts.

Footnotes

[27] "Built-in Fleet Intelligence: The Bottom Line," Telogis.com, accessed June 30, 2015, http://www.telogis.com/gm.

[28] Jana Winter and Sharon Weinberger, "Sensitive Military Gear Ended up on Craigslist," *The Intercept*, March 26, 2015, https://firstlook.org/theintercept/2015/03/26/missing-military-tech-ended-ebay-craiglist.

[29] "Nest Thermostat: Saving Energy," Nest.com, accessed June 30, 2015, https://nest.com/thermostat/saving-energy/

[30] U.S. Department of Defense, "Department of Defense Annual Energy Management Report Fiscal Year 2014," 18

[31] Adam Mazmanian, "It Takes DISA 3.5 Hours to Activate a Single Classified Mobile Phone—Here's Why," FCW.com, October 22, 2014, http://fcw.com/articles/2014/10/22/disa-classified-mobile-phone.aspx.

[32] U.S. Department of Defense, Office of the Chief Information Officer, "The Department of Defense Strategy for Implementing the Joint Information Environment," September 18, 2013, http://dodcio.defense.gov/Portals/0/Documents/JIE/2013-09-13_DoD_Strategy_for_Implmenting_JIE_%28NDAA_931%29_Final_Document.pdf.

OceanofPDF.com

Appendix: Subject-Matter Experts Interviewed

We would like to thank the subject-matter experts interviewed as part of the research for this project. While the findings and recommendations in this report were informed by these interviews, they should not be viewed as having been endorsed by the experts we interviewed.

LIEUTENANT COLONEL BRIAN AMEND
Supply and Logistics Officer, U.S. Marine Corps

MAJOR RYAN BAKER
Supply and Logistics Officer, U.S. Marine Corps

FRANK BOURNE
Chief Scientist, Government Communications Systems, Harris Corporation

VERN BOYLE
Director of Technology, Cyber Division, Northrop Grumman Information Systems

GENERAL JAMES CARTWRIGHT
Harold Brown Chair in Defense Policy Studies, CSIS; Former Vice Chairman of Joint Chiefs of Staff

MAJOR MICHELLE CHARLESTON
Commander, Defense Logistics Agency

JAMES CROWLEY
Chief of Staff, Global Risk Advisors, and Former Member, U.S. Army Special Operations Command

TED DANG
Engineer/Scientist Adaptive Execution office, DARPA

WILLIAM GREENWALT
Professional Staff Member, Senate Armed Services Committee

RICHARD A. HALE
Deputy Chief Information Officer for Cyber Security, Department of Defense

BRIAN KEMPER
Chief Engineer, Program Manager, Training Devices (PM-TRADE), Program Executive Office for Simulation, Training, and Instrumentation (PEO STRI)

JOHN KRIZ
Senior Scientist, Test and Evaluation for Aircraft Systems, Avionics, and Weapons, NAVAIR

MICHAEL LACK
Senior Research Director and Deputy General Manager, Invincea Labs

JEREMY T. LANMAN, PH.D.
Lead Systems Architect, Program Manager, Training Devices (PM-TRADE), Program Executive Office for Simulation, Training, and Instrumentation (PEO STRI)

LIEUTENANT COLONEL MICHAEL MASTRIA
Supply and Logistics Officer, U.S. Marine Corps

MICHAEL MAY
Science and Engineering Lead, Assistant Secretary of Defense for Research and Engineering

MICHAEL MCGINLEY
Engagement Officer, USCYBERCOM

MUKESH MEHTA
Marketing Manager, AT&T Government Solutions

DAVID MIHELCIC
Chief Technology Officer and Principal Director, Global Information Grid Enterprise Services Engineering, Defense Information Systems Agency

JOHN NAGENGAST
Director of Government Relations, AT&T

CAPTAIN HANNAH PAXTON
Logistics and Finance Director, U.S. Marine Corps Expeditionary Warfare, Pacific

DAVID POWELL
Managing Director, UK Office, Global Risk Advisors

JACQUELYN SCHNEIDER
Graduate Student, Political Science, The George Washington University

NEIL SIEGEL
Sector Vice President and Chief Technology Officer, Northrop Grumman Corporation

CHRIS SMITH

Vice President of Technology, AT&T Government Solutions

JAMES TODD
Lead Systems Engineer/PD/COR, Science and Technology Lead, Program Manager, Training Devices (PM-TRADE), Program Executive Office for Simulation, Training, and Instrumentation (PEO STRI)

MAJOR GENERAL JOHN WHARTON
U.S. Army Research, Development, and Engineering Program

GREG YOUST
Chief Mobility Engineer, Technology and Integration Division, Chief Technology Office, Defense Information Systems Agency

OceanofPDF.com

Further Reading

1. Connie Albrecht et al., “Fleet Management of Tactical Wheeled Vehicles,” *Army AL&T*, July–September, 2010: 25–27, http://asc.army.mil/docs/pubs/alt/archives/2010/Jul-Sep_2010.pdf.
2. AT&T, “Leveraging the Power of Connected Machines,” Presentation AT&T M2M Business Solutions, 2014, http://vertassets.blob.core.windows.net/download/fb378057/fb378057-53f1-4ff5-87c7-c62770e9c864/m2m_from_att_pharma.pdf.
3. Battelle, “2014 Global R&D Funding Forecast,” December 2013, http://www.battelle.org/docs/tpp/2014_global_rd_funding_forecast.pdf .
4. Black Diamond, “Advancements in Wearable Computing Solutions Aid JTAC Missions,” BDAT White Paper, 2011, http://bdatech.com/files/resources/BDAT-MTS-JTAC-White-paper-SCREEN.pdf.
5. Angelina Long Callahan, “Reinventing the Drone, Reinventing the Navy: 1919–1939,” *Naval War College Review 67*, no. 3 (2014): 98–122, https://www.usnwc.edu/getattachment/52d53799-ce32-4a36-bb08-2425c045167a/Reinventing-the-Drone,-Reinventing-the-Navy--1919-.aspx.
6. Cisco, “Enabling the Global Defense Mission,” Cisco Solution Overview, 2007, http://www.cisco.com/web/strategy/docs/gov/C22-428943-00_CiscoDefenseExecutiveSummary_FINAL.pdf.
7. Cisco, “Transforming How Government Serves, Protects and Defends,” Cisco Global Government Solutions and Services, 2007, http://www.cisco.com/web/strategy/docs/gov/GovSolsSvcs_C02-423837-00_072908.pdf.
8. Cisco, “Cisco Classified Network Support,” Cisco Data Sheet, 2012, http://www.cisco.com/web/strategy/docs/gov/datasheet_c78_698310_v

3.pdf.

9. Cisco, “Internet of Everything Capabilities for the U.S. Navy,” Cisco White Paper, 2015, http://www.cisco.com/web/strategy/us_government/resources/navy-ioe-wp1c.pdf.
10. “Command, Control, Communications, Computers and Intelligence (C4I) Systems and Capability Set 13,” *Army Magazine 62*, no. 10 (2012): 333–42, http://www.ausa.org/publications/armymagazine/archive/2012/10/Documents/Weapons3_1012.pdf.
11. Kevin Deal, “Why Aerospace and Defense Maintenance Needs Mobile MRO,” IFS White Paper, May 2013, http://www.ifsworld.com/de/~/media/assets/2014/09/12/13/46/white-papers-why-aerospace-and-defense-needs-mobile-mro.pdf.
12. Defense Information Systems Agency, “Global Combat Support System—Joint Program Overview,” August 2014, www.disa.mil/Mission-Support/Command-and-Control/GCSS-J/Program-Overview-Brief.
13. Entrust, “Defending the Internet of Things: Identity at the Core of Security,” Entrust White Paper, 2014, http://www.entrust.com/wp-content/uploads/2014/09/WP_Entrust-IOT_Sept2014.pdf.
14. David Evans, “Introducing the Wireless Cow,” Politico.com, June 2015, http://www.politico.com/agenda/story/2015/06/internet-of-things-growth-challenges-000098.
15. Andrew Feickert, “The Unified Command Plan and Combatant Commands: Background and Issues for Congress,” Congressional Research Service, January 3, 2013, https://www.fas.org/sgp/crs/natsec/R42077.pdf.
16. Inventure FMS Gateway, “Fleet Management System Standard (FMS Standard),” Accessed June 30, 2015, http://fmsgateway.com/glossary/fleet-management-system-standard-fms-standard.

17. General Dynamics, “Tactical Ground Reporting (TIGR) System,” TIGR Handout, 2012, http://www.gdc4s.com/Documents/Programs/TIGR%20Handout-Final.pdf.

18. Bill Gertz, “General: Strategic Military Satellites Vulnerable to Attack in Future Space War,” *Washington Free Beacon*, January 8, 2014, http://freebeacon.com/national-security/general-strategic-military-satellites-vulnerable-to-attack-in-future-space-war/.

19. Jacob L. Hall II and Major Christopher Buckham, “In Transit Visibility: A Tool to Enhancing the Military Decision-making Process,” *Defense Transportation Journal*, June 2014: 12–15, http://www.ndtahq.com/documents/In_Transit_Visibility_000.pdf.

20. Harbor Research, “Smart Systems Manifesto: Road Map for the Internet of Things,” White paper, September 2013, http://harborresearch.com/wp-content/uploads/2013/09/HRI_Paper_Smart-Sys-Manifesto.pdf.

21. John Hickey, “DoD Mobility Overview,” Presentation by the DoD Mobility Portfolio Manager at the Joint Information Environment Mission Partner Symposium 2014, Baltimore, MD, May 14, 2014, http://www.afcea.org/events/jie/14/documents/DoDMobilityHickeyFinal1.pdf.

22. Wayne P. Hughes, “Naval Operations: A Close Look at the Operational Level of War at Sea,” *Naval War College Review 65*, no. 3 (2012): 23–47.

23. “Individual Equipment and Weapons,” *Army Magazine 60*, no. 10 (2010): 364–73, http://www.ausa.org/publications/armymagazine/archive/2010/10/Documents/Weapons7_Individual_1010.pdf.

24. James Kadtke and Linton Wells II, “Policy Challenges of Accelerating Technological Change: Security Policy and Strategy Implications of Parallel Scientific Revolutions,” Center for Technology and National Security Policy, National Defense University, September, 2014, http://ctnsp.dodlive.mil/files/2014/09/DTP106.pdf.

25. James Macaulay, Lauren Buckalew, and Gina Chung, “Internet of Things in Logistics,” Collaborative report by Cisco Consulting Services and DHL Trend Research, 2015, http://www.dhl.com/content/dam/Local_Images/g0/New_aboutus/innovation/DHLTrendReport_Internet_of_things.pdf.

26. Northrop Grumman, “Communications, Navigation and Identification (CNI) Avionics for the F-35 Lightning II,” CNI Data Sheet, 2012, http://www.northropgrumman.com/Capabilities/SDRs/Documents/F35-CNI_datasht.pdf.

27. Admiral Williams A. Owens, “The Emerging U.S. System-of-Systems,” *Strategic Forum 63* (1996): 1–6, http://www.dtic.mil/cgi-bin/GetTRDoc?AD=ADA394313.

28. “Phalanx Close-In Weapon System,” Raytheon.com, Accessed June 29, 2015, http://www.raytheon.com/capabilities/products/phalanx.

29. Monica Paolini, “Wireless Security in LTE Networks,” Senza Fili Consulting, 2012, http://www.gsma.com/membership/wp-content/uploads/2012/11/SenzaFili_Wirelesssecurity_121029_FINAL.pdf.

30. 30. Qualcomm, “LTE Advanced—Evolving and Expanding into New Frontiers,” August 2014, https://www.qualcomm.com/documents/lte-advanced-evolving-and-expandingnew-frontiers.

31. Alex Rossino, “Observations from TTC’s Internet of Things for Defense Symposium,” *GovWin* (blog), November 25, 2014, https://iq.govwin.com/index.cfm?fractal=blogTool.dsp.blog&blogname=public&alias=Observations-from-TTCs-Internet-of-Things-for-Defense-Symposium.

32. Moshe Schwartz, “Defense Acquisitions: How DOD Acquires Weapon Systems and Recent Efforts to Reform the Process,” Congressional Research Service, May 23, 2014, https://www.fas.org/sgp/crs/natsec/RL34026.pdf.

33. George I. Seffers, “Defense Department Awakens to Internet of Things,” *Signal Magazine*, last modified January 1, 2015, http://www.afcea.org/content/?q=defense-department-awakens-internet-things.

34. Deric Sims, “DoD Non Tactical Vehicle Fleet Management,” DoD Fleet Manager Presentation on OUSD(AT&L)/ARA [Office of the Under Secretary of Defense for Acquisition, Technology and Logistics/Acquisition Resources and Analysis] Property and Equipment Policy, Accessed June 29, 2015, http://www.acq.osd.mil/pepolicy/pdfs/DoD_Non_Tactical_Vehicle.pdf.

35. Dennis Steele, “Setting the Azimuth for Joint Force 2020: Globally Integrated Operations and Mission Command,” *Army Magazine 62*, no. 11 (2012): 27–29, http://www.ausa.org/publications/armymagazine/archive/2012/11/Documents/Steele_1112.pdf.

36. Chris Sweeney, Liu Liu, Sean Arietta, and Jason Lawrence, “HIPI: A Hadoop Image Processing Interface for Image-based MapReduce Tasks,” Undergraduate thesis, University of Virginia, 2011, https://cs.ucsb.edu/~cmsweeney/papers/undergrad_thesis.pdf.

37. Telit Wireless Solutions, “LTE & The IoT—M2M Environment,” June 2014, http://www.telit.com/fileadmin/user_upload/media/telit_lte-m2m_wp.pdf.

38. John F. Troxell, “2014–15 Key Strategic Issues List,” Strategic Studies Institute, October 31, 2014, http://www.strategicstudiesinstitute.army.mil/index.cfm/articles/2014-15-KSIL/2014/06/17.

39. U.S. Army, Program Executive Office Soldier, “Equipment Portfolio 2014,” Accessed June 29, 2015, www.peosoldier.army.mil/portfolio/#1.

40. U.S. Chairman of the Joint Chiefs of Staff, “CJCS Guide to the Chairman’s Readiness System,” CJCS Guide 3401D, November 15, 2010, http://www.dtic.mil/cjcs_directives/cdata/unlimit/g3401.pdf.

41. U.S. Chairman of the Joint Chiefs of Staff, “Joint Information Environment White Paper,” January 22, 2013, http://www.jcs.mil/Portals/36/Documents/Publications/environmentalwhitepaper.pdf.

42. U.S. Chairman of the Joint Chiefs of Staff, “2014–2017 Chairman’s Joint Training Guidance,” CJCS Notice 3500.01, October 10, 2013,

http://sapr.mil/public/docs/news/CJCS_Notice3500_01.pdf.

43. U.S. Chairman of the Joint Chiefs of Staff, "Joint Capabilities Integration and Development System," CJCS Instruction 3170.01I, January 23, 2015, http://www.dtic.mil/cjcs_directives/cdata/unlimit/3170_01a.pdf.

44. U.S. Department of Defense, "Department of Defense Information Technology Enterprise Strategy and Roadmap," September 6, 2011, http://dodcio.defense.gov/Portals/0/Documents/Announcement/Signed_ITESR_6SEP11.pdf.

45. U.S. Department of Defense, "Condition Based Maintenance Plus (CBM^{+}) for Materiel Maintenance," Department of Defense Instruction 4151.22, October 16, 2012, http://www.dtic.mil/whs/directives/corres/pdf/415122p.pdf.

46. U.S. Department of Defense, "Serialized Item Management (SIM) for Life-Cycle Management of Materiel," Department of Defense Instruction 4151.19, January 9, 2014, http://www.dtic.mil/whs/directives/corres/pdf/415119p.pdf.

47. U.S. Department of Defense, "Quadrennial Defense Review 2014," March 4, 2014, http://www.defense.gov/pubs/2014_Quadrennial_Defense_Review.pdf.

48. U.S. Department of Defense, "Fiscal Year 2013 Operational Energy Annual Report," October 15, 2014, http://energy.defense.gov/Portals/25/Documents/Reports/FY13%20OE%20Annual%20Report.pdf.

49. U.S. Department of Defense, "The Department of Defense Cyber Strategy," April 17, 2015, http://www.defense.gov/home/features/2015/0415_cyber-strategy/Final_2015_DoD_CYBER_STRATEGY_for_web.pdf.

50. U.S. Department of Defense, Office of the Chief Information Officer, "Volume I: Management Overview of the DoD IEA," Department of Defense Information Enterprise Architecture, Version 2.0, July 2012, http://dodcio.defense.gov/Portals/0/Documents/DIEA/DoD%20IEA%

20v2.0_Volume%20I_Description%20Document_Final_20120730.pdf
.

51. U.S. Department of Defense, Office of the Chief Information Officer, “Volume II: IEA Description,” Department of Defense Information Enterprise Architecture, Version 2.0, July, 2012, http://dodcio.defense.gov/Portals/0/Documents/DIEA/DoD%20IEA%20v2%200_Volume%20II_Description%20Document_Final_20120806.pdf.
52. U.S. Department of Defense, Office of the Chief Information Officer, “Cloud Computing Strategy,” July 2012, http://www.defense.gov/news/DoDCloudComputingStrategy.pdf.
53. U.S. Department of Defense, Office of the Director Operational Test and Evaluation, “Air Force Distributed Common Ground Segment,” *FY 2010 Annual Report for the Office of the Director Operational Test & Evaluation*, December 2010, 181–2, http://www.dote.osd.mil/pub/reports/FY2010/pdf/af/2010afdcgs.pdf.
54. U.S. Department of Defense, Office of the Director Operational Test and Evaluation, “Defense Readiness Reporting System,” *FY 2013 Annual Report for the Office of the Director Operational Test & Evaluation*, January 2014, 31–32, http://www.dote.osd.mil/pub/reports/FY2013/pdf/dod/2013drrs.pdf.
55. U.S. Department of Defense, Office of the Inspector General, “Defense Information Systems Agency’s Acquisition Management of the Global Combat Support System,” DOD Audit Report D-2000-142, June 9, 2000, http://www.dodig.mil/audit/reports/fy00/00-142.pdf.
56. U.S. Department of Defense, Office of the Inspector General, “Allegations Unsubstantiated Concerning Defense Logistics Agency Violation of Federal Guidance for the Maintenance, Repair, and Operations Contracts,” DODIG-2013-143, September 30, 2013, http://www.dodig.mil/pubs/documents/DODIG-2013-143.pdf.
57. U.S. Department of Defense, Office of the Inspector General, “Army Needs to Improve the Reliability of the Spare Parts Forecasts It Submits to the Defense Logistics Agency,” DODIG-2014-124,

September 29, 2014, http://www.dodig.mil/pubs/documents/DODIG-2014-124.pdf.

58. U.S. Department of Defense, Office of the Inspector General, "DoD Needs to Reinitiate Migration to Internet Protocol Version 6," DODIG-2015-044, December 1, 2014, http://www.dodig.mil/pubs/documents/DODIG-2015-044.pdf.
59. U.S. Defense Logistics Agency, "Military Making for Shipment and Storage," MIL-STD-129P w/CHANGE #4, 2008, http://www.landandmaritime.dla.mil/downloads/packaging/129p_chg4_08_mc.pdf.
60. U.S. Defense Logistics Agency, 2012 Director's Guidance, April 2012, http://www.dla.mil/Documents/DLA_2012_DG_web.pdf.
61. U.S. Defense Logistics Agency, "Fleet Management Plan FY 2013," March 1, 2013, http://www.dla.mil/InstallationSupport/InstallationManagement/Documents/FY13%20FINAL%20DLA%20FMP%20Adobe.pdf.
62. U.S. Defense Logistics Agency, *Fleet Newsletter*, no. 3 (2014), http://www.dla.mil/InstallationSupport/InstallationManagement/Documents/DLA%20Fleet%20Newsletter3_Spring2014.pdf.
63. U.S. Defense Logistics Agency, "Implementation Plan for Adopting Office of the Secretary of Defense's Defense Property and Accountability System Fleet Management Information System," Version 2.0, December 18, 2014, http://www.dla.mil/Installationsupport/InstallationManagement/Documents/FinalDLADPASFMISImplementationPlan-18Dec2014.pdf.
64. U.S. Government Accountability Office, "Federal Vehicle Fleets: Adopting Leading Practices Could Improve Management," Report to the Ranking Member Committee on the Budget, U.S. Senate, GAO-12-659, July 2013, http://www.gao.gov/assets/660/656444.pdf.
65. U.S. Government Accountability Office, "Acquisition Reform: DoD Should Streamline Its Decision-Making Process for Weapon Systems to Reduce Inefficiencies," Report to Congressional Committees, GAO-15-192, February 2015, http://www.gao.gov/assets/670/668629.pdf.

66. U.S. Government Accountability Office, “Defense Acquisitions: Assessments of Selected Weapon Programs,” Report to Congressional Committees, GAO-15-342SP, March 2015, http://www.gao.gov/assets/670/668986.pdf.

67. U.S. Marine Corps, “Marine Corps Installations and Logistics Roadmap,” June 20, 2013, http://www.iandl.marines.mil/Portals/85/Docs/Division%20LP%20Documents/MCILR_lowres_June20-1.pdf.

68. U.S. Marine Corps, “Marine Corps Logistics IT Portfolio Strategy,” 2014, http://www.iandl.marines.mil/Portals/85/Docs/Division%20LP%20Documents/Log%20IT%20Portfolio%20Strategy.pdf.

69. Verizon, “Connected Solutions Overview for Department of Defense Customers,” Verizon White Paper, 2014, http://www.verizonenterprise.com/industry/public_sector/federal/m2m/wp16168_m2m_dod.pdf.

70. Tim Wickham and August Cole, “Why the Pentagon and the Defense Industry Need to Engage Silicon Valley,” *National Defense Magazine Blog*, January 5, 2015, http://www.nationaldefensemagazine.org/blog/Lists/Posts/Post.aspx?ID=1707.

71. Wind River, “The Internet of Things for Defense,” Wind White Paper, 2015, http://www.windriver.com/whitepapers/iot-for-defense/wind-river_%20IoT-in-Defense_ white-paper.pdf.

72. Admiral James A. Winnefeld Jr., Remarks at the Joint Service Academy Cyber Security Summit hosted by the U.S. Military Academy, West Point, NY, May 14, 2014, http://www.jcs.mil/Media/Speeches/tabid/3890/Article/589135/adm-winnefelds-remarks-atthe-west-point-cyber-conference.aspx.

73. World Economic Forum and Accenture, “Industrial Internet of Things: Unleashing the Potential of Connected Products and Services,” January 2015, http://www3.weforum.org/docs/WEFUSA_IndustrialInternet_Report2015.pdf.

74. Xerafy, “Military Usage of Passive RFID,” Xerafy White Paper, Accessed June 29, 2015, http://www.xerafy.com/userfiles/misc/resources/whitepapers/Military%20Usage%20of%20RFID%20Whitepaper.pdf.

75. Greg Youst, “DoD’s Strategic Mobility Vision: Needs & Challenges,” Presentation for the Security Management & Assurance group at NIST, October 22, 2014, http://csrc.nist.gov/groups/SMA/ispab/documents/minutes/2014-10/oct22_dod_mobility-needs-and-challenges_youst.pdf.

OceanofPDF.com

About the Authors

Denise E. Zheng is a senior fellow and deputy director of the Strategic Technologies Program at CSIS, where her work is focused on technology, innovation, and cybersecurity and Internet policy. Previously, she served as chief of staff and lead science and engineering technical adviser as a contractor for the Defense Advanced Research Projects Agency (DARPA) foundational cyber warfare program, Plan X. Before DARPA, Ms. Zheng was director for global government relations and cybersecurity policy at CA Technologies, a $5 billion enterprise software company, where she advised company executives on cybersecurity, data security and breach notification, and software assurance. While at CA, Ms. Zheng was a member of the Information Technology (IT) Sector Coordinating Council, IT Information Sharing and Analysis Center, SAFECode, and vice chair of the TechAmerica Cybersecurity Legislative Subcommittee. Ms. Zheng holds a B.A. in economics and political science from the University of Michigan, studied government at the London School of Economics and Political Science, and completed graduate coursework in security studies at the Johns Hopkins University School of Advanced International Studies

William A. Carter is a research associate in the Strategic Technologies Program at CSIS. Before joining CSIS in January 2015, he worked as a financial analyst in the Goldman Sachs Investment Strategy Group, advising private and institutional clients on their short- to medium-term asset allocation decisions. In this role, he performed research and analysis on all investable asset classes, as well as geopolitics and the macro economy, and produced reports and presentations on international affairs and current events. He has interned at the Council on Foreign Relations and at Caxton Associates, a New York hedge fund. He graduated from New York University in 2010 with a B.A. in economics.

OceanofPDF.com